Module code: M303 **Further Pure Mathematics**

Practice Quizzes

Contents

1. Practice Quiz 1
2. Practice Quiz 2
3. Practice Quiz 3
4. Practice Quiz 4
5. Practice Quiz 5
6. Practice Quiz 6

SUP088160

SUP088160

The Open University

M303

Further pure mathematics

Practice Quiz 1

Question 1

Use the Euclidean Algorithm to determine $\text{hcf}(133, 49)$.

Question 2

Find the least positive integer x for the linear Diophantine equation:

$$260x + 148y = 4.$$

Question 3

The highest common factor of:

$2^2 \times 3^2 \times 5 \times 7 \times 13^4$ and $3^2 \times 5^2 \times 11^3 \times 17$ is x, and the lowest common multiple is y, where x and y are as follows:

Select one or more:

The hcf is $x = 3^2 \times 5$ and the lcm is $y = 2^2 \times 3^2 \times 5^2 \times 7 \times 11^3 \times 13^4 \times 17$

The hcf is $x = 3^2 \times 5$ and the lcm is $y = 2^2 \times 3^4 \times 5^3 \times 7 \times 11^3 \times 13^4 \times 17$

The hcf is $x = 2 \times 3 \times 5 \times 7$ and the lcm is $y = 2^2 \times 3^4 \times 5^3 \times 7 \times 11^3 \times 13^4 \times 17$

The hcf is $x = 2 \times 3 \times 5 \times 7$ and the lcm is $y = 2^2 \times 3^2 \times 5^2 \times 7 \times 11^3 \times 13^4 \times 17$

The hcf is $x = 3 \times 5$ and the lcm is $y = 2^3 \times 3^2 \times 5^2 \times 7 \times 11^3 \times 13^4 \times 17$

The hcf is $x = 3 \times 5$ and the lcm is $y = 2^2 \times 3^2 \times 5^2 \times 7 \times 11^3 \times 13^4 \times 17$

Question 4

How many distinct factors does the number $55191641225 = 5^2 \times 7^3 \times 23^5$ have?

Question 5

Is the statement below true or false?

$$36 \equiv 3 \pmod{11}?$$

Question 6

This question asks you to work in $\mathbb{Z}_{11} = \{[0], [1], \ldots, [10]\}$.

What is n where $[n] = [10] + [8]$ in $\mathbb{Z}_{11}$?

Question 7

This question asks you to work in $\mathbb{Z}_{14} = \{[0], [1], \ldots, [13]\}$.

What is n where $[n] = [9] \times [7]$ in $\mathbb{Z}_{14}$?

Question 8

Drag and drop the correct phrases into the appropriate boxes to make the following into true statements. [is] [is not]

The solution to the linear congruence $14x \equiv 7 \pmod{13}$ [ ] unique.

The solution to the linear congruence $7x \equiv 21 \pmod{14}$ [ ] unique.

The solution to the linear congruence $13x \equiv 13 \pmod{14}$ [ ] unique.

Question 9

Calculate the smallest non-negative value for x that satisfies the linear congruence below.

$$16 \times x \equiv 14 \pmod{11}$$

Question 10

Find the least positive integer x that simultaneously satisfies the three congruences:

$$x \equiv 1 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$

and

$$x \equiv 1 \pmod{4}.$$

Question 11

Which of the following statements can be deduced directly from Fermat's Little Theorem or the alternative formulation.

Select one or more:

$$13^{11} \equiv 1 \pmod{10}$$
$$130^{10} \equiv 1 \pmod{11}$$
$$49^{7} \equiv 7 \pmod{7}$$
$$99^{10} \equiv 1 \pmod{11}$$
$$15^{4} \equiv 15 \pmod{5}$$
$$21^{7} \equiv 21 \pmod{7}$$

Question 12

Find the least positive residue of $15^{67} \pmod{23}$.

Question 13

What is the degree of the polynomial congruence

$$25x^8 + 16x^3 + 3x^2 \text{ modulo } 5?$$

Question 14

Select the missing words to make the following statements correct.

If p is prime and d is a factor of $p-1$ then the congruence $x^d - 1 \equiv 0 \pmod{p}$ has d solutions where $d =$ exactly, less than or more than.

If a and b are positive integers with $\text{hcf}(a, b) = 1$ then there are d many primes of the form $ak + b$ where k is a non-negative integer where $d =$ finitely or infinitely.

Solutions

Solution to Question 1

The correct answer is 7.

We begin by dividing the larger number, 133, by the smaller number, 49, which gives us a remainder 35.

$$133 = 2 \times 49 + 35$$

Next we divide 49 by the remainder 35

$$49 = 1 \times 35 + 14$$

and then we continue, at each stage dividing the previous factor by the resulting remainder

$$35 = 2 \times 14 + 7$$
$$14 = 2 \times 7 + 0$$

until we obtain a remainder of 0 and the algorithm stops.

In this case we see that 7 is the highest common factor of 133 and 49 and the algorithm, written in full, is:

$$133 = 2 \times 49 + 35$$
$$49 = 1 \times 35 + 14$$
$$35 = 2 \times 14 + 7$$
$$14 = 2 \times 7 + 0$$

See Chapter 1, Section 5.1 and in particular, Worked Exercise 5.1.

Solution to Question 2

The correct answer is 4.

We follow the method of Worked Exercise 5.3 of Book A, Chapter 1 (page 45).

We first note that we can simplify $260x + 148y = 4$ by dividing through by 4 to give the 'same' equation $65x + 37y = 1$. We run the Euclidean Algorithm to calculate $\text{hcf}\,(65, 37)$.

$$65 = 1 \times 37 + 28$$
$$37 = 1 \times 28 + 9$$
$$28 = 3 \times 9 + 1$$
$$9 = 9 \times 1 + 0$$

This shows that hcf (65,37)=1 and so Theorem 5.4 of Book A Chapter 1 (HB page 16) tells us that $260x + 148y$ has solutions.

We now reverse the equations from the Euclidean Algorithm to give the following:

$$\begin{aligned} 1 &= 28 - (3 \times 9) \\ &= 28 - 3(37 - (1 \times 28)) \\ &= -(3 \times 37) + (4 \times 28) \\ &= -(3 \times 37) + 4(65 - (1 \times 37)) \\ &= (4 \times 65) + (-7 \times 37). \end{aligned}$$

This expresses 1 as an integer combination of 65 and 37. However we wanted 4 as an integer combination of 260 and 148 so we multiply through by 4 to get:

$$4 = (4 \times 260) + (-7 \times 148)$$

so $x = 4,\ y = -7$ is one solution to the equation $260x + 148y = 4$.

We now use Theorem 5.4 of Book A, Chapter 1 (HB page 16) to write the general solution for x as:

$$x = 4 + 37k,\ y = -7 - 65k,\ k \in \mathbb{Z}.$$

By inspection we see that the least positive value for x is 4.

Solution to Question 3

By the formula below Proposition 2.1 in the HB (page 17) we have the following:

if the prime decomposition of M and N is given by $M = p_1^{k_1} \dots p_r^{k_r}$ and $N = p_1^{l_1} \dots p_r^{l_r}$ then $\text{hcf}\,(M, N) = p_1^{\min\{k_1,l_1\}} \dots p_r^{\min\{k_r,l_r\}}$ and $\text{lcm}\,(M, N) = p_1^{\max\{k_1,l_1\}} \dots p_r^{\max\{k_r,l_r\}}$.

Therefore the hcf is $x = 3^2 \times 5$ and the lcm is $y = 2^2 \times 3^2 \times 5^2 \times 7 \times 11^3 \times 13^4 \times 17$

Note that if a prime, p_i, does not appear in the prime factorisation of a number $N = p_1^{l_1} \dots p_r^{l_r}$ then the exponent, l_i, is taken to be zero.

See Proposition 2.1, Exercise 2.2 and the box below Exercise 2.2 of Book A, Chapter 2 (pages 79 and 80).

Solution to Question 4

The correct answer is 72.

The number of distinct factors is given by the τ function (Definition 2.2 Chapter 2, HB page 17).

The formula $\tau(n) = (k_1 + 1) \times \cdots \times (k_r + 1)$ where $n = p_1^{k_1} \cdots p_r^{k_r}$ (see Proposition 2.3 of Chapter 2, HB page 17)

Since $55191641225 = 5^2 \times 7^3 \times 23^5$, the number of distinct factors of 55191641225 is

$$(2 + 1)(3 + 1)(5 + 1) = 72.$$

See Book A, Chapter 2, page 82.

Solution to Question 5

This is true since $36 - 3 = 3$ and $33 = 3 \times 11$ (by Definition 1.1 of Chapter 3, HB page 18)

Solution to Question 6

The correct answer is 7.

$10 + 8 = 18$ so we want to calculate n where 18 is in the residue class $[n]$ modulo 11, and $0 \leq n \leq 10$. Therefore we need the smallest non-negative number, n, where $18 \equiv n \pmod{11}$. That is we need the smallest non-negative number n such that $18 = n + 11k$ for some k.

By direct calculation we can see that $18 = 7 + (1 \times 11)$. Therefore $n = 7$.

See Book A, Chapter 3, Section 1.2 and, in particular, Exercise 1.4 (pages 132 - 134).

Solution to Question 7

The correct answer is 7.

$9 \times 7 = 63$ so we want to calculate n where 63 is in the residue class $[n]$ modulo 14, and $0 \leq n \leq 13$. Therefore we need the least non-negative number, n, where $63 \equiv n \pmod{14}$. That is we need the smallest non-negative number n such that $63 = n + 14k$ for some k.

By direct calculation we can see that $63 = 7 + (4 \times 14)$. Therefore $n = 7$.

See Book A, Chapter 3, Section 1.2 and, in particular, Exercise 1.4 (pages 132 - 134).

Solution to Question 8

The $\text{hcf}(14, 13) = 1$ and so the congruence $14x \equiv 7 \pmod{13}$ has a unique solution (by Theorem 3.4, HB page 20).

The $\text{hcf}(7, 14) = 7$ and 7 divides 21 so the congruence $7x \equiv 21 \pmod{14}$ has 7 solutions (by Theorem 3.4, HB page 20).

The $\text{hcf}(13, 14) = 1$ and so the congruence $13x \equiv 13 \pmod{14}$ has a unique solution (by Theorem 3.4, HB page 20).

Solution to Question 9

Since $\text{hcf}(16, 11) = 1$ this congruence has a unique solution modulo 11 (by Theorem 3.4 Chapter 3, HB page 20)

The following gives one way of solving this question.

Subtracting 1×11 from 16 gives

$$5 \times x \equiv 14 \pmod{11}.$$

Adding 1×11 to 14 gives

$$5 \times x \equiv 25 \pmod{11}$$

Since $25 = 5 \times 5$, and 5 is coprime to 11 , we can divide through by 5 (by Corollary 1.9 of Chapter 3, HB page 19) to get

$$x \equiv 5 \pmod{11}.$$

Hence the smallest positive value for x that satisfies the original congruence is $x = 5$.

See Worked Exercise 3.5 of Chapter 3 (page 148 of Book A), and the strategy on page 20 of the handbook, for more details.

Solution to Question 10

The answer is 13.

The easiest way to do this kind of question is often 'by inspection'. In other words by writing out the first few classes which contain the numbers satisfying each individual congruence, and looking for the least integer common to all 3 sets.

Taking each congruence in turn we have the following.

The congruence $x \equiv 1 (\text{mod } 4)$ is satisfied by all numbers in the sequence

$$1, 5, 9, 13, 17, 21, \ldots, 4n + 1, \ldots$$

The congruence $x \equiv 3 \,(\text{mod } 5)$ is satisfied by all numbers in the sequence

$$3, 8, 13, 18, 23, 28, 33, \ldots, 5n + 3 \ldots$$

The congruence $x \equiv 1 \,(\text{mod } 3)$ is satisfied by all numbers in the sequence

$$1, 4, 7, 10, 13, 16, 19, \ldots, 3n + 1, \ldots$$

and so, by inspection, we see that the least positive integer that simultaneously satisfies the three congruences

$x \equiv 1 \,(\text{mod } 3)$

$x \equiv 3 \,(\text{mod } 5)$

and

$x \equiv 1 \,(\text{mod } 4)$ is 13.

See Book A, Chapter 3, pages 156 and 157, Worked Exercise 4.4.

Note that if this method does not work easily then simultaneous linear congruences can always be solved using the Chinese Remainder Theorem, which is Theorem 4.2 of Chapter 3, page 153 (HB page 20), but it is usually worth trying to solve them by inspection first.

Solution to Question 11

Theorem 1.1 of Book A Chapter 4, page 181, (HB page 21) states that if p is prime and a is any integer with $\text{hcf}\,(a, p) = 1$ then $a^{(p-1)} \equiv a \,(\text{mod } p)$. The alternative formulation (HB page 21 or Chapter 4 page 182) states that for any integer a and prime p we have $a^p \equiv a \,(\text{mod } p)$.

$99^{10} \equiv 1 \,(\text{mod } 11)$ and since $\text{hcf}\,(99, 11) \neq 1$ this cannot be deduced from Fermat's Little Theorem (HB page 21) since the exponent is not equal to the modulus we cannot directly apply the alternative formulation.

$130^{10} \equiv 1 \,(\text{mod } 11)$: since $\text{hcf}\,(130, 11) = 1$, and 11 is prime, this can be deduced directly from Fermat's Little Theorem, (HB page 21).

$13^{11} \equiv 1 \,(\text{mod } 10)$: since 10 is not prime neither Fermat's Little Theorem nor the alternative formulation apply here.

$49^7 \equiv 1 \,(\text{mod } 7)$: since this expression is not of the form $a^{p-1} \equiv 1$, or of the form $a^p \equiv a$, the equation cannot be deduced directly from either Fermat's Little Theorem or its alternative formulation (HB page 21).

$15^4 \equiv 15 \,(\text{mod } 5)$: since this expression is not of the form $a^{p-1} \equiv 1$, or of the form $a^p \equiv a$, for a prime p, the equation cannot be deduced directly from either Fermat's Little Theorem or its alternative formulation (HB page 21).

$21^7 \equiv 21 \,(\text{mod } 7)$: this follows from the alternative formulation of Fermat's Little Theorem (HB page 21).

Solution to Question 12

The least residue of $15^{67} \,(\text{mod } 23)$ is 15.

Since 23 is prime and $\text{hcf}\,(15, 23) = 1$ we can use Fermat's Little Theorem (HB page 21) which tells us that $15^{22} \equiv 1 (\text{mod } 23)$.

Now $67 = 22 \times 3 + 1$ and so we have:

$$\begin{aligned} 15^{67} &= 15^{(22\times 3+1)} \\ &= (15^{22})^3 \times 15^1 \\ &\equiv 1^3 \times 15^1 \,(\text{mod } 23) \\ &\equiv 15^1 \equiv 15 \,(\text{mod } 23). \end{aligned}$$

Since the least positive residue (Section 1.2 of Book A Chapter 3, page 132) of $15 \,(\text{mod } 23)$ is 15 the solution is 15.

See Book A, Chapter 4, Page 183, Worked Exercise 1.2

Solution to Question 13

To calculate the degree of a polynomial congruence modulo 5, we first remove each term in which the coefficient is congruent to $0 \pmod 5$ (Definition 4.2 of Chapter 4, HB page 22). Therefore since $25 \equiv 0 \pmod 5$, we remove the term involving x^8 and the degree of the polynomial congruence

$25x^8 + 16x^3 + 3x^2$ modulo 5 is 3.

For more details see Book A, Chapter 4, Page 201.

Solution to Question 14

By Proposition 4.8 of Book A Chapter 4, (HB page 22) if p is prime and d is a factor of $p - 1$ then the congruence has exactly d solutions.

By Theorem 3.5 of Book A Chapter 2 (Dirichlet's Theorem, HB page 18) if a and b are positive integers with $\text{hcf}(a, b) = 1$ then there are infinitely many primes of the form $ak + b$, where k is a non-negative integer.

The Open University

M303

Further pure mathematics

Practice Quiz 2

Question 1

Let G be the group
$G = (\{1, 3, 5, 9, 11, 13\}, \times_{14})$.

Select the 4 true statements from the following list.

- G is generated by the element 3
- 11 is an element of order 3
- G is not abelian
- G is generated by the element 9
- G is cyclic
- $\langle 13 \rangle$ is a cyclic subgroup of order 2
- $\langle 11 \rangle$ is a cyclic subgroup of order 2

Question 2

Find the following product in S_6 in cycle form and select the correct option.

$(1\,2\,3\,4\,5)(1\,6)$

Select one.

- $(1\,2\,4\,6\,3\,5)$
- $(1\,2\,3\,6\,4\,5)$
- $(1\,2\,3\,4\,5\,6)$
- $(1\,4\,5\,6\,2\,3)$
- $(1\,3\,5\,6\,2\,4)$
- $(1\,6\,2\,3\,4\,5)$

Question 3

Fill the blank spaces below to correctly complete the statements.

It is [ ] that an abelian subgroup is always normal.

All subgroups of an abelian group are [ ].

Question 4

Let G be the following subgroup of S_6 of order 16:

$G = \{e, (1\,2), (3\,5), (4\,6), (1\,2)(3\,5), (1\,2)(4\,6), (3\,5)(4\,6), (3\,4)(5\,6), (3\,6)(4\,5), (3\,4\,5\,6), (3\,6\,5\,4), (1\,2)(3\,5)(4\,6), (1\,2)(3\,4)(5\,6), (1\,2)(3\,6)(4\,5), (1\,2)(3\,4\,5\,6), (1\,2)(3\,6\,5\,4)\}$

Let H and J be the following subgroups of G of orders 8 and 4 respectively:

$H = \{e, (3\,5), (4\,6), (3\,5)(4\,6), (3\,4)(5\,6), (3\,6)(4\,5), (3\,4\,5\,6), (3\,6\,5\,4)\}$

$J = \{e, (3\,5), (4\,6), (3\,5)(4\,6)\}$

In each of the options below, the first statement is true, but the *deduction* "**so**..." leading to the conclusion may or may not follow from this statement. You are asked to determine the validity of this *deduction* and not the truth of the final conclusion, which may or may not be true.

Select the 2 options with a correct *deduction* from the following list.

Let $g = (1\,2)(3\,4\,5\,6)$, then $g(4\,6)g^{-1} \neq (4\,6)$ and **so** the left and right cosets of J in G are not equal.

The left and right cosets of J in G are equal, **so** J is normal in G.

There are four left cosets of J in G and there are four right cosets of J in G, **so** J is normal in G.

The index of J in H is 2, **so** J is normal in H.

J is normal in H, and H is normal in G, **so** J is normal in G.

$g(3\,5)(4\,6)g^{-1} = (3\,5)(4\,6)$ for all $g \in G$, **so** J is normal in G.

Question 5

Select the 2 true statements from the following list.

$\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{15}$ is cyclic

$\mathbb{Z}_3 \times \mathbb{Z}_{18} \cong \mathbb{Z}_{54}$

$\mathbb{Z}_{14} \times \mathbb{Z}_{41}$ is cyclic

$\mathbb{Z}_{20} \times \mathbb{Z}_{35}$ is cyclic

$\mathbb{Z}_3 \times \mathbb{Z}_{16} \cong \mathbb{Z}_{45}$

$\mathbb{Z}_5 \times \mathbb{Z}_{12} \cong \mathbb{Z}_{60}$

Question 6

Select the 2 true statements from the following list.

The element (2,3) generates $\mathbb{Z}_3 \times \mathbb{Z}_8$

The element (2,5) generates $\mathbb{Z}_3 \times \mathbb{Z}_{12}$

$\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ has a subgroup of order 12

$\mathbb{Z}_3 \times \mathbb{Z}_8$ has a subgroup of order 9

$\mathbb{Z}_2 \times \mathbb{Z}_8 \cong \mathbb{Z}_{16}$

$\mathbb{Z}_3 \times \mathbb{Z}_{12} \cong \mathbb{Z}_6 \times \mathbb{Z}_6$

Question 7

In which 2 of the following groups is the greatest order of an element 6?

$\mathbb{Z}_3 \times \mathbb{Z}_8$

$\mathbb{Z}_2 \times \mathbb{Z}_4$

$\mathbb{Z}_3 \times S_4$

$\mathbb{Z}_3 \times S_3$

$\mathbb{Z}_2 \times A_4$

$\mathbb{Z}_4 \times A_4$

Question 8

Let G be a group and X be a non-empty set with G acting on X by $\wedge$.

Let the elements x and y be in the set X.

Select the 2 true statements from the following list.

$x \neq y$ implies that $\text{Orb}(x) \neq \text{Orb}(y)$

$\text{Stab}(x) = \text{Stab}(y)$ implies that $\text{Send}_x(y) = \text{Send}_y(x)$

$\text{Orb}(x) \cap \text{Orb}(y) = \phi$ implies there is a $g \in G$ such that $g \wedge x = y$

$g \in \text{Send}_x(y)$ implies $g^{-1} \wedge y = x$

$g \in \text{Stab}(y)$ and $h \in \text{Send}_x(y)$ implies $hg \wedge y = x$

$g \wedge x = x$ implies that $g^{-1} \wedge x = x$

Question 9

Which 2 of the following describe the dihedral group D_6?

$\langle r, s | r^6 = e, s^2 = e, srs = r \rangle$

$\{r^i : i = 0, 1, \ldots, 5, r^6 = e\}$

$\langle r, s | r^6 = e, s^2 = e, sr = r^{-1}s \rangle$

$\langle a, b \rangle \subseteq S_6$, where $a = (1\,2\,3\,4\,5\,6)$ and $b = (1\,4)(2\,5)(3\,6)$

$\langle a, b \rangle \subseteq S_6$, where $a = (1\,2\,3\,4\,5\,6)$ and $b = (1\,2)(3\,6)(4\,5)$

$\langle r, s | r^4 = e, r^2 = s^6, rs^3rs = e \rangle$

Question 10

Let G be the dihedral group D_6, so

$$G = \langle r, s | r^6 = s^2 = e, sr = r^5 s \rangle.$$

Select the 2 true statements from the following list.

r is conjugate to r^3

$\text{Cent}_{D6}(r^3) = \{e, r, r^2, r^3, r^4, r^5\}$

r^2 is conjugate to r^5

$\text{Cent}_{D6}(r^2) = \{e, r, r^2, r^3, r^4, r^5\}$

r^2 is conjugate to $r^2 s$

$\text{Cent}_{D6}(r^3 s) = \{e, r^3, r^3 s, s\}$

$r^2 s$ is conjugate to $r^3 s$

Question 11

Let G be the dicyclic group Dic_4, so

$$G = \langle a, b | a^4 = e, a^2 = b^4, aba^3 b = e \rangle.$$

Select the 2 true statements from the following list.

$\langle b \rangle$ is a subgroup of order 4.

$ba^3 = a^3 b$.

$Z(G) = \{e, a^2\}$.

$b^3 a^3 = ab$.

$\text{Cent}_G(a^2) = \{e, a^2\}$.

Question 12

Consider the matrices

$$A = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

in the multiplicative group of invertible 2×2 matrices with entries in $\mathbb{C}$.

Let G be the group generated by A and B, which you may assume has order 8.

Select one:

G is isomorphic to $\mathbb{Z}_8$

G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$

G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

G is isomorphic to D_4

G is isomorphic to Dic_2

Question 13

Write in the correct expressions from the list below (you may use a given expression more than once) to complete the proof of the following proposition.

Proposition

The centre of any non-abelian group of order 70 has order at most 7.

Proof

Let G be a non-abelian group of order 70 with centre Z. We assume to the [ ] that Z has order greater than [ ]. Now, Z is a [ ] of G, so [ ] implies that its order divides [ ] and so the possible orders of Z are 10, 14, [ ] or 70. However, since G is [ ], the order of Z is not [ ]. We consider the quotient G/Z which must have order 7, [ ] or 2. In any of the three cases this [ ] has [ ] order and so is [ ], and hence G would be [ ] by [ ] (Chapter 7, HB page 36) giving the required contradiction. Therefore the centre has order at most 7.

Choices

5, 7, 35, 70, abelian, contrary, cyclic, Lagrange's Theorem, non-abelian, prime, quotient, subgroup, Theorem 2.14

Question 14

Fill in the correct numbers below to complete the statements.

Let G be a group of order 225. The Sylow Theorems (Chapter 8, Theorem 1.12, HB page 39) imply the following

- G has m_3 Sylow 3-subgroups, where $m_3 \equiv 1 \pmod{\square}$ and m_3 divides $\square$, so $m_3 = \square$;
- G has m_5 Sylow 5-subgroups, where $m_5 \equiv 1 \pmod{\square}$ and m_5 divides $\square$, so $m_5 = \square$.

Question 15

The following are all abelian groups of order 700.

Choose the two options that represent the same group (up to isomorphism).

$\mathbb{Z}_{28} \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_{14} \times \mathbb{Z}_{50}$

$\mathbb{Z}_{700}$

$\mathbb{Z}_{14} \times \mathbb{Z}_{10} \times \mathbb{Z}_5$

$\mathbb{Z}_{20} \times \mathbb{Z}_{35}$

Question 16

Let G be a group of order $48 = 2^4 \times 3$.

Let m_2 and m_3 be the numbers of Sylow 2-subgroups and 3-subgroups, as permitted by the Sylow Theorems.

Let H be a Sylow 2-subgroup and K be a Sylow 3-subgroup of G.

From the list below, select the 3 statements that can be deduced from the Sylow Theorems.

$|H|$ may be 2, 4, 8 or 16

$m_2 \equiv 1 (\text{mod } 16)$ and m_2 divides 3, so m_2 is 1

$m_3 \equiv 1 (\text{mod } 3)$ and m_3 divides 2, so m_3 is 1

$m_2 \equiv 1 (\text{mod } 2)$ and m_2 divides 3, so m_2 is 1 or 3$|H| = 16$ and $|K| = 3$

$m_3 \equiv 1 (\text{mod } 3)$ and m_3 divides 16, so m_3 is 1, 4 or 16

Question 17

Up to isomorphism, how many abelian groups of order 250 are there?

Question 18

Let G be a non-abelian group of order 26.

How many subgroups of order 2 does G have?

Solutions

Solution to Question 1

The correct answer is:

G is cyclic

$\langle 13 \rangle$ is a cyclic subgroup of order 2

G is generated by the element 3

11 is an element of order 3

Multiplication modulo 14 is commutative and so G is an abelian group.

G is also cyclic of order 6; it is generated by either one of the elements 3 and 5. (*Order of a group*, Chapter 5, Definition 2.15.)

The elements 9 and 11 have order 3 and the element 13 has order 2. (*Order of an element*, Chapter 5, Definition 4.4.)

Solution to Question 2

The correct answer is:

$(1\,6\,2\,3\,4\,5)$

Products of permutations are described in Chapter 5, Subsection 1.2.

A fully worked example is given in the solution to Chapter 5, Exercise 1.5(c).

Solution to Question 3

It is false that an abelian subgroup is always normal.

All subgroups of an abelian group are normal.

An abelian subgroup is not always normal. A subgroup H of a group G is abelian if $hk = kh$ for all h and k in H. This condition only gives us information about the elements inside the subgroup H. A subgroup $H \subseteq G$ is normal if $gH = Hg$ for all g in G. This condition of being normal involves all elements of G, not just elements of the subgroup H. Normal subgroups are not always abelian and abelian subgroups are not always normal. An example is given by considering the subgroup $\{e, (12)\}$ of S_3.

If the *whole group* G is abelian, then $ag = ga$ for every $a \in G$ and $g \in G$. Therefore we must have $aH = Ha$ for any subgroup H. In other words subgroups of abelian groups are always normal (see Chapter 5, Definition 3.6 (HB page 27)). Abelian groups are defined on HB page 23. See also Exercise 3.2 of Chapter 5.

A cyclic group is a special kind of abelian group and subgroups of an abelian group are not always cyclic. Any group is a subgroup of itself and so the Klein group $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is an example of a non-cyclic subgroup of the abelian group V, see HB page 23.

Solution to Question 4

The correct answer is:

The left and right cosets of J in G are equal, **so** J is normal in G.

The index of J in H is 2, **so** J is normal in H.

It is important to be able to determine whether, or not, a given subgroup is a *normal* subgroup. Normality is defined in Chapter 5, Definition 3.6 (HB page 27) and normality can be proved using this definition directly, however, Propositions 3.7, 3.10 and 3.12 (HB pages 27 and 28) all give alternative ways of proving normality. Different methods may be more straightforward to use than others depending on the groups involved. (*Normal subgroups*, Chapter 5, Subsection 3.1.)

One crucial fact to understand is that $gNg^{-1} = N$ does not imply that $gng^{-1} = n$ for any given $n \in N$, only that gng^{-1} is some element in N.

Two useful facts to remember are (Chapter 5, Exercise 3.3(b) and (c)):

- A subgroup of index 2 is necessarily normal
- The intersection of normal subgroups of G is normal in G.

Let H and M be the following subgroups of G of orders 8 and 4, respectively:

$$H = \{e, (1\,2), (3\,5), (4\,6), (1\,2)(3\,5), (1\,2)(4\,6), (3\,5)(4\,6), (1\,2)(3\,4)(5\,6)\}$$

$$M = \{e, (1\,2), (3\,5), (1\,2)(3\,5)\}$$

You might like to check that M is normal in H and that H is normal in G, but that M is not normal in G.

Solution to Question 5

The correct answer is:

$\mathbb{Z}_{14} \times \mathbb{Z}_{41}$ is cyclic

$\mathbb{Z}_5 \times \mathbb{Z}_{12} \cong \mathbb{Z}_{60}$

It is important to master the art of determining when a direct product of *cyclic* groups is cyclic (*Direct products of cyclic groups*, Chapter 6, Theorem 2.11 and Corollary 2.12, HB page 32).

Solution to Question 6

The correct answer is:

$\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_4$ has a subgroup of order 12

The element (2,3) generates $\mathbb{Z}_3 \times \mathbb{Z}_8$

It is important to be able to decompose a *cyclic* group into a product of cyclic groups of prime power order (*Decomposition of finite cyclic groups*, Chapter 6, Theorem 2.13, HB page 32 and Exercise 2.11).

It is equally important to be able to determine whether or not two direct products of cyclic groups (i.e. two abelian groups) are isomorphic. To prove they are isomorphic, show that they are both isomorphic to the same product of cyclic groups of prime power order. They are not isomorphic if, for example, their elements of highest order have different orders.

Given any direct product $G = A \times B$, the order of an element $(a, b) \in G$, is the least common multiple of the orders of a and b, respectively, in the groups A and B (Chapter 6, Proposition 2.8, HB page 32).

Given an element g of order n in G, the subgroup generated by g is a cyclic group of order n (*Cyclic groups*, Chapter 5, Definition 1.8, HB page 25).

Solution to Question 7

The correct answers are:

$\mathbb{Z}_3 \times S_3$

$\mathbb{Z}_2 \times A_4$

Cauchy's Theorem states that there is an element of each prime order dividing the order of a group (*Cauchy's Theorem*, Chapter 6, Theorem 3.16, HB page 34).

Given any direct product $G = A \times B$, the order of an element $(a, b) \in G$, is the lowest common multiple of the orders of a and b, respectively, in the groups A and B (Chapter 6, Proposition 2.8, HB page 32).

Knowledge of small groups such as these provides an important source of counter-examples, especially the non-abelian ones formed from the direct product of a cyclic group and a non-abelian group.

Solution to Question 8

The correct answer is:

$g \wedge x = x$ implies that $g^{-1} \wedge x = x$

$g \in \mathrm{Send}_x(y)$ implies $g^{-1} \wedge y = x$

Group actions provide a powerful tool in group theory. For example, they are used to prove Cayley's Theorem and Cauchy's Theorem (Chapter 6, Theorems 3.15 and 3.16, HB pages 33 and 34) and the Sylow Theorems (Chapter 8, Theorem 1.12, HB page 39).

A group action of G on a set X determines an equivalence relation on the set X (Chapter 6, Proposition 3.8, HB page 33), where two elements of the set X are equivalent if they are in the same orbit; that is, there is an element of G that sends one to the other.

It is important to remember what type of elements make up orbits, stabilisers and send:

- An orbit is a subset of elements of the set X being acted upon
- A stabiliser is a subgroup of the group G doing the acting
- Send is a subset of the group G doing the acting; it is, in fact, a coset of a stabiliser

Solution to Question 9

The correct answers are:

$\langle r, s | r^6 = e, s^2 = e, sr = r^{-1}s \rangle$

$\langle a, b \rangle \subseteq S_6$, where $a = (1\,2\,3\,4\,5\,6)$ and $b = (1\,2)(3\,6)(4\,5)$

Groups can be described in a variety of ways using generators and relations; a group may look quite different in different guises.

For example, the dihedral group D_6 can be thought of with the elements in standard form $r^i s^j$ or equally well as permutations on the six corners of a regular hexagon. It is useful to be able to recognise groups from their presentations (*Generators and relations*, Chapter 7, Subsection 1.1).

Solution to Question 10

The correct answers are:

$\text{Cent}_{D6}(r^2) = \{e, r, r^2, r^3, r^4, r^5\}$

$\text{Cent}_{D6}(r^3 s) = \{e, r^3, r^3 s, s\}$.

Conjugate elements share many properties, for example, they have the same order and in a symmetry group, such as D_6, they are the same "type" of symmetry; that is, they are both rotations or reflections, and further if they are reflections they both fix two vertices or both fix no vertices (*Conjugacy*, Chapter 7, Definition 2.3, Proposition 2.5, Exercise 2.2, the hints given above Exercise 2.2, or HB page 35).

The centraliser of an element a is the set of elements that conjugate a to itself. Both e and a will be in the centraliser of a, along with all the elements that commute with a (*Centraliser*, Chapter 7, Definition 2.7, Exercise 2.3, or HB page 36).

The centre of a group is the set of central elements, those that commute with all other elements. It is the union of the single element conjugacy classes and any element a in the centre has $\text{Cent}_G = G$. (Chapter 7, Definition 2.8, Proposition 2.10, Exercise 2.7, or HB page 36.)

Solution to Question 11

The correct answers are:

$b^3 a^3 = ab$

$Z(G) = \{e, a^2\}$

Working in a dicyclic group provides excellent practice in manipulating group elements given by a presentation (*Dicyclic groups*, Chapter 7, Subsection 1.2). The more you practise the easier it becomes!

The elements need to be simplified into the standard form (Chapter 7, Exercise 1.8), in this case

$$a^r b^s \text{ for } r = 0, \ldots, 3, \text{ and } s = 0, \ldots, 3.$$

It is useful to remember, in particular, that in $ba = a^3 b^{n-1}$, so in this case, $ba = a^3 b^3$.

Solution to Question 12

The correct answer is:

G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$

Groups of order 8 are investigated in Chapter 7, Subsection 3.4, and Theorem 3.6 (HB page 37) guarantees that G is isomorphic to one of the five groups of order 8 listed.

If $AB = BA$, then G is abelian, since if the generators of a group commute, then all elements of the group will commute.

If G is abelian and has

- 1 element of order 2, then G is isomorphic to $\mathbb{Z}_8$
- 3 elements of order 2, then G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$
- 7 elements of order 2, then G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

If $AB \neq BA$ then G is non-abelian.

If G is non-abelian and has

- 5 elements of order 2, then G is isomorphic to D_4
- 1 element of order 2, then G is isomorphic to Dic_2

In this case, $AB = BA$ so G is abelian. In addition, the elements A, B^2 and AB^2 have order 2, and B, B^3, AB and AB^3 have order 4, so G is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Solution to Question 13

Let G be a non-abelian group of order 70 with centre Z. We assume to the contrary that Z has order greater than 7. Now, Z is a subgroup of G, so Lagrange's Theorem implies that its order divides 70 and so the possible orders of Z are 10, 14, 35 or 70. However, since G is non-abelian, the order of Z is not 70. We consider the quotient G/Z which must have order 7, 5 or 2. In any of the three cases this quotient has prime order and so is cyclic, and hence G would be abelian by Theorem 2.14 (Chapter 7, HB page 36) giving the required contradiction. Therefore the centre has order at most 7.

Solution to Question 14

The correct statement is

Let G be a group of order 225. The Sylow Theorems (Chapter 8, Theorem 1.2, HB page 39) imply the following:

- G has m_3 Sylow 3-subgroups, where $m_3 \equiv 1 \pmod 3$ and m_3 divides 25, so $m_3 = 1$ or 25
- G has m_5 Sylow 5-subgroups, where $m_5 \equiv 1 \pmod 5$ and m_5 divides 9, so $m_5 = 1$.

Finding the possible numbers of Sylow subgroups provides valuable insight into a group. Indeed with this information it is possible to go on and show powerful results ... for example, that all groups of a given order are cyclic, abelian or cannot be simple.

Solution to Question 15

The correct answer is:

$\mathbb{Z}_{28} \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20} \times \mathbb{Z}_{35}$.

Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders (Chapter 8, Theorem 2.2, HB page 39).

To compare groups, it is advisable to write them in this form, collecting all the cyclic groups for the same prime together, within parenthesis.

Remember, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if m and n are coprime (*Direct product of cyclic groups*, Chapter 6, Theorem 2.11 and Corollary 2.12, HB page 32) and therefore, prime power cyclic components, for the same prime, cannot be combined together into one component.

Solution to Question 16

The correct answer is:

A group of order 48 has

$m_2 \equiv 1 (\mathrm{mod}\ 2)$ and m_2 divides 3,
so m_2 is 1 or 3

$m_3 \equiv 1 (\mathrm{mod}\ 3)$ and m_3 divides 16,
so m_3 is 1, 4 or 16

$|H| = 16$ and $|K| = 3$.

The Sylow Theorems (Chapter 8, Theorem 1.12, HB page 39) state that a group G of order $p^\alpha z$ has
$m_p \equiv 1 (\mathrm{mod}\ p)$, and m_p divides z.

Note that this second condition is equivalent to m_p divides $|G|$, but it is usually easier to use z as the numbers are smaller!

The definition of a Sylow p-subgroup gives its order as p^α (*Sylow p-subgroup*, Chapter 8, Definition 1.7, HB page 38).

It is really important to master being able to determine the numbers of Sylow subgroups; once you get the hang of it, it is quite straightforward!

Solution to Question 17

Every finite abelian group can be expressed as a direct product of abelian groups of prime power order, one for each prime dividing the order (*Finite abelian groups*, Chapter 8, Theorem 2.2, HB page 39, and Exercise 2.1).

Here, $250 = 2 \times 5^3$ so $G = H \times K$ where $|H| = 2$ and $|K| = 125$.

There is just one possibility for H and three for K giving **three** groups in total.

The three groups are:

$\mathbb{Z}_2 \times (\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5)$

$\mathbb{Z}_2 \times (\mathbb{Z}_5 \times \mathbb{Z}_{25})$

$\mathbb{Z}_2 \times \mathbb{Z}_{125}$

Solution to Question 18

The correct answer is: 13.

Note that arguments like this are dependent on the order of the group involved. For example, when $|G| = 12$ we have three non-isomorphic non-abelian groups: D_6, A_4 and Dic_3 (by Chapter 7, Theorem 3.11, HB page 37). It turns out that both D_6 and Dic_3 have three Sylow 2-subgroups, but A_4 has a unique (and hence normal) Sylow 2-subgroup; it has four Sylow 3-subgroups.

We note that $26 = 2 \times 13$.

The Sylow Theorems (Chapter 8, Theorem 1.12, HB page 39) give:

the number of Sylow 2-subgroups is congruent to 1 (mod 2) and divides 13, and so is 1 or 13;

the number of Sylow 13-subgroups is congruent to 1 (mod 13) and divides 2, and so is 1.

If there is a unique Sylow subgroup for each order, then these Sylow subgroups are normal (Chapter 8, Lemma 1.9, HB page 39).

In addition, their orders are coprime and the product of their orders is the order of G, so they form an internal direct product (Chapter 8, Theorem 2.3, HB page 39).

This direct product of two prime order groups is necessarily abelian, and hence ruled out by G being non-abelian.

Therefore there must be 13 Sylow 2-subgroups, the only other possibility.

The Open University

M303

Further pure mathematics

Practice Quiz 3

Question 1

What is the value of $\phi(168)$?

Question 2

Calculate $\sigma(38)$ directly from the definition.

Question 3

Use the table below to calculate $\tau(60)$.

n	1	2	3	4	5	6	7	8	9	10
τ(n)	1	2	2	3	2	4	2	4	3	4

Question 4

Which of the following can be deduced from results in the text, without calculating the value of $\phi(n)$ for any number n?

Select one or more:

$\phi(10 \times 9) = \phi(10) \times \phi(9)$
$\phi(36) = (\phi(2))^2 \times (\phi(3))^2$
$\phi(121 + 130) = \phi(121) + \phi(130)$
$\phi(121 \times 130) = \phi(121) \times \phi(130)$
$\phi(81) = (\phi(3))^4$

Question 5

Find the least positive residue of 338^{102} modulo 33.

The least residue of 338^{102} modulo 33 is $\square$.

Question 6

Which three of the following are quadratic residues modulo 7?

Select one or more:

1
2
3
4
5
6

Question 7

Use Euler's Criterion to answer the following question.

Is it true or false that 3 is a quadratic residue of 29?

Select one:

True

False

Question 8

Is the following true or false? Select the correct answer.

Let $f(x) = (x + \frac{1}{2})(x - \frac{1}{2})$. Then $f = gh$, with $g, h \in \mathbb{Q}[x]$ and so, by Gauss' Lemma (that is Theorem 4.13 of Chapter 11, HB page 52) we can write $f = GH$ with $G, H \in \mathbb{Z}[x]$.

Select one:

True

False

Question 9

What is the value of the Legendre symbol (50/43)?

Question 10

Calculate (975/43) (note that $975 = 25 \times 13 \times 3$)

Question 11

Use the rational root test to answer the following question.

It is [ ] that the polynomial $f(x) = x^3 + 3x^2 + 4x - 2$ is reducible over $\mathbb{Q}[x]$.

Question 12

It is [ ] that Eisenstein's criterion shows that the polynomial $f(x) = x^4 + 3x^3 + 21x^2 - x + 9$ is irreducible over $\mathbb{Q}[x]$.

Question 13

Let R be a commutative ring. We say that a non-zero element $x \in R$ is [ ] if $x|yz$, for $y, z \in R$, implies that either $x|y$ or $x|z$.

Let R be a commutative ring. If a non-zero element $x \in R$ can be written as a product, $x = yz$, with y, z non-units in R, then we say that x is [ ].

Question 14

This question is about $\mathbb{Z}_{11}$.

Which of the following is true. Select all that apply.

- $\mathbb{Z}_{11}$ is a ring (with addition and multiplication defined modulo 11).
- $\mathbb{Z}_{11}$ is a field.
- $\mathbb{Z}_{11}$ is an integral domain.
- Every non-zero element of $\mathbb{Z}_{11}$ has a multiplicative inverse (under multiplication modulo 11).
- The elements $\{0, \ldots, 10\}$ of $\mathbb{Z}_{11}$ form a cyclic group under addition modulo 11.

Question 15

Determine which of 'True' or 'False' should be written in the blank space.

It is [ ] that the number $5945113699 = 19^5 \times 7^4$ can be expressed as the sum of two squares.

Solutions

Solution to Question 1

The value of $\phi(168)$ is 48.

We have $168 = 2^3 \times 3^1 \times 7^1$, so the Alternative formula for $\phi(n)$ given in Book C, Chapter 9, Page 35 (HB page 44) tells us that

$$\begin{aligned}\phi(168) &= 2^2 \times 3^0 \times 7^0 \times (2-1)(3-1)(7-1)\\ &= 4 \times 1 \times 1 \times 2 \times 6\\ &= 48.\end{aligned}$$

You could also use the formula given in Proposition 4.2 of Chapter 9 (HB page 44).

See Exercise 4.2 and Worked Exercise 4.3 on page 34 of Chapter 9.

Solution to Question 2

The sum of the divisors of 38 is 60.

The sum of divisors function σ is given by

$$\sigma(n) = \sum_{d|n} d,$$

where the sum is over all the divisors of n (Definition 1.2, Chapter 9, HB page 42).

In this case, the divisors of 38 are $\{1, 2, 19, 38\}$, which add up to 60.

Solution to Question 3

The value of $\tau(60)$ is 12.

We have $60 = 2^2 \times 3^1 \times 5$. Since τ is multiplicative (Corollary 1.6 of Chapter 9, HB page 42) we have that

$$\begin{aligned}\tau(2^2 \times 3^1 \times 5) &= \tau(2^2) \times \tau(3^1) \times \tau(5)\\ &= \tau(4) \times \tau(3) \times \tau(5)\\ &= 3 \times 2 \times 2\\ &= 12.\end{aligned}$$

Solution to Question 4

The first, second and fourth statements can be deduced.

Euler's ϕ-function is multiplicative so for any two coprime integers n and m we have $\phi(n \times m) = \phi(n) \times \phi(m)$ by Definition 1.2, Proposition 1.4 and Theorem 4.2 of Chapter 9 (HB pages 42 and 44). See also Exercise 4.1 on page 33 of Chapter 9.

Note that it is not true that $\phi(n \times m) = \phi(n) \times \phi(m)$ when n and m are not coprime.

Solution to Question 5

The least residue of 338^{102} modulo 33 is 31.

First, $338 \equiv 8 \pmod{33}$ and so $338^{102} \equiv 8^{102} \pmod{33}$ by Theorem 1.2(f) of Chapter 3 (HB page 19).

Since $\text{hcf}(8, 33) = 1$, Euler's Theorem (which is Theorem 3.3 of Chapter 9, HB page 43) tells us that $8^{\phi(33)} \equiv 1 \pmod{33}$.

So we first need to calculate $\phi(33)$.

Using the fact that ϕ is multiplicative (Theorem 4.1 of Chapter 9, HB page 44) and the Alternative formula for ϕ (HB page 44) we have:

$$\begin{aligned}\phi(33) &= \phi(3 \times 11)\\ &= \phi(3) \times \phi(11)\\ &= 2 \times (11-1)\\ &= 20.\end{aligned}$$

Therefore, $8^{20} \equiv 1 \pmod{33}$.

Since $102 = 5 \times 20 + 2$, we have

$$338^{102} \equiv 8^{102} = (8^{20})^5 \times (8)^2 \equiv (8)^2 \pmod{33}.$$

Thus $8^2 = 64 \equiv 31 \pmod{33}$, which gives the result.

See Book C, Chapter 9, Page 27, Worked Exercise 3.7

Solution to Question 6

By Definition 2.1 of Chapter 10 (HB page 45) a number $a \neq 0 \pmod 7$ is a quadratic residue modulo 7 if we can find a number x such that $x^2 \equiv a \pmod 7$. Therefore we can find the quadratic residues of 7 simply by squaring all the numbers up to 7 and reducing the result modulo 7.

Since:

$$1^2 \equiv 1 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$4^2 \equiv 2 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$6^2 \equiv 1 \pmod 7$$

we see that 1, 2 and 4 are the quadratic residues modulo 7.

See Chapter 10, Page 64, Worked Exercise 1.3.

Note that since $(-x)^2 = x^2$ it is only necessary to square the first three numbers since $a^2 \equiv (7-a)^2 \pmod 7$.

There are other ways to do this question. For example it is also possible to use Theorem 1.5, Euler's Criterion (HB page 45).

See Chapter 10, Page 69, Worked Exercise 1.6.

Solution to Question 7

A number, a, is a quadratic residue modulo p if we can find an x such that $x^2 = a \pmod p$ (Definition 1.2 of Chapter 10, HB page 45).

It is, of course, possible to determine all the quadratic residues and non residues modulo p by simply squaring numbers modulo p and looking at the results; but we can also use results such as Euler's Criterion (Theorem 1.5 of Chapter 10, HB page 45).

Euler's Criterion states that a number, a, not congruent to 0 modulo p is a quadratic residue for an odd prime p if, and only if, $a^{(p-1)/2} \equiv 1 \pmod p$.

To use Euler's Criterion we need to calculate $3^{14} \pmod{29}$.

Noticing that $3^3 = 27$ and $27 \equiv -2 \pmod{29}$ we proceed as follows:

$$\begin{aligned} 3^{14} &\equiv (3^3)^4 \times 9 \pmod{29} \\ &\equiv (-2)^4 \times 9 \pmod{29} \\ &\equiv 16 \times 9 \pmod{29} \\ &\equiv 144 \pmod{29} \\ &\equiv -1 \pmod{29} \end{aligned}$$

Therefore, by Euler's Criterion, we see that it is **false** that 3 is a quadratic residue modulo 29.

Solution to Question 8

This is **false**.

This does not follow from Gauss' Lemma (that is Theorem 4.13 of Chapter 11, HB page 52) since $f(x) = x^2 - \frac{1}{4} \notin \mathbb{Z}[x]$. To apply Gauss' Lemma you must start with a polynomial, $f(x)$, in $\mathbb{Z}[x]$.

Solution to Question 9

Since $50 = 25 \times 2$ and $25 = 5^2$ is a square number, we have

$$(50/43) = 1 \times (2/43) = 1 \times -1 = -1.$$

See Book C, Chapter 10, Theorem 2.2 and Proposition 3.2 (HB page 46).

Solution to Question 10

The answer is -1.

We have:

$$(975/43) = (25/43) \times (13/43) \times (3/43)$$

since the Legendre symbol is multiplicative by Theorem 2.2 of Chapter 10 (HB page 46).

Now $(25/43) = (5^2/43) = 1$ by Theorem 2.2 of Chapter 10 (HB page 46).

In addition, since $43 \equiv 7 \pmod{12}$, the result on the quadratic character of 3 (HB page 46) gives $(3/43) = -1$.

Therefore

$$(975/43) = 1 \times (13/43) \times -1.$$

So we need to calculate $(13/43)$. The Law of Quadratic Reciprocity (alternative formulation – Theorem 4.2 of Chapter 10, HB page 46) tells us that

$$(13/43) = 1 \times (43/13)$$ (since both 13 and 43 are odd primes with $43 \equiv 3 \pmod 4$ and $13 \equiv 1 \pmod 4$).

Therefore, since $43 \equiv 4 \pmod{13}$ we have $(13/43) = 1 \times (43/13) = 1 \times (4/13) = 1$ by Theorem 2.2(a) and (b) (HB page 46).

Therefore

$$\begin{aligned}(975/43) &= 1 \times 1 \times 1 \times -1 \\ &= -1.\end{aligned}$$

Solution to Question 11

True

Since $f(x)$ has degree 3, if $f(x)$ has any factors then one of these must be a linear factor. We use the rational root test, that is Theorem 4.7 of Chapter 11 (HB page 52), to determine whether $f(x)$ has any linear factors.

The polynomial $f(x)$ is a polynomial in $\mathbb{Z}[x]$ so the rational root test tells us that any rational root $\frac{p}{q} \in \mathbb{Q}$ of $f(x)$ with $\text{hcf}(p, q) = 1$ must be such that p is an integer factor of -2 and q an integer factor of 1. This means that p must be ± 2 or ± 1, and q must be ± 1. Therefore the only possible roots are ± 2 or ± 1. We can check each of these by substituting these four values into the polynomial in turn.

We have:

- $f(2) = 26$ and so 2 is not a root (Definition 4.1 of Chapter 11, HB page 51). Therefore by the Factor Theorem (that is Theorem 4.2 of Chapter 11) we see that $(x - 2)$ is not a factor.
- $f(-2) = -6$ and so -2 is not a root (Definition 4.1 of Chapter 11, HB page 51). Therefore by the Factor Theorem (that is Theorem 4.2 of Chapter 11) we see that $(x + 2)$ is not a factor.
- $f(1) = 6$ and so 1 is not a root (Definition 4.1 of Chapter 11, HB page 51). Therefore by the Factor Theorem (that is Theorem 4.2 of Chapter 11) we see that $(x - 1)$ is not a factor.
- $f(-1) = -4$ and so -1 is not a root (Definition 4.1 of Chapter 11, HB page 51). Therefore by the Factor Theorem (that is Theorem 4.2 of Chapter 11) we see that $(x + 1)$ is not a factor.

Therefore $f(x)$ is irreducible.

Solution to Question 12

False

Eisenstein's criterion (Theorem 4.15 of Chapter 11, HB page 52) tells us that the polynomial $f(x) \in \mathbb{Z}[x]$, is irreducible over $\mathbb{Q}[x]$ if we can find a prime, p, such that:

(i) p divides the constant term and the coefficients of x, x^2 and x^3, but does not divide the coefficient of x^4, and

(ii) p^2 does not divide the constant term.

Looking at $f(x)$ we see that the coefficient of x^2 is $21 = 7 \times 3$. Therefore our only choices for the prime p are 3 or 7. Now the prime p must also divide the constant term, 9, but 7 clearly does not divide 9. Therefore the only possibility is $p = 3$.

We check the conditions for each coefficient in turn.

- The prime 3 divides the constant term 9, but the square 9 divides 9, so this does not satisfy the conditions for Eisenstein's criterion.

- The prime 3 does not divide -1, the coefficient of x, so this does not satisfy the conditions for Eisenstein's criterion.
- By design, the prime 3 divides the coefficient of x^2, so this satisfies the conditions for Eisenstein's criterion.
- The prime 3 divides 3, the coefficient of x^3, so this satisfies the conditions for Eisenstein's criterion.
- The prime 3 does not divide 1, the coefficient of x^4, so this satisfies the conditions for Eisenstein's criterion.

Therefore Eisenstein's criterion cannot be used to deduce that $f(x)$ is irreducible.

Note that we do not need to check all of the conditions to deduce that Eisenstein's criterion cannot be used here, it is sufficient to find one case where the conditions are not met.

Solution to Question 13

The correct answers are as follows.

Let R be a commutative ring. We say that a non-zero element $x \in R$ is **prime** (Definition 2.6 of Chapter 12, HB page 54) if $x|yz$, for y, $z \in R$, implies that either $x|y$ or $x|z$.

Let R be a commutative ring. If a non-zero element $x \in R$ can be written as a product, $x = yz$, with y, z non-units in R, then we say that x is **reducible** (see Definition 2.5 of Chapter 12, HB page 54).

Solution to Question 14

The elements $\{0, \ldots, 10\}$ of $\mathbb{Z}_{11}$ form a cyclic group under addition modulo 11 (Theorem 2.1 of Chapter 6, HB page 31).

$\mathbb{Z}_{11}$ is a ring (Exercise 1.2 of Chapter 11, page 114).

$\mathbb{Z}_{11}$ is a field by Corollary 1.19 of Chapter 11 (HB page 49).

Since $\mathbb{Z}_{11}$ is a field (Corollary 1.19 of Chapter 11, HB page 49), it has no zero divisors (Lemma 1.17 of Chapter 11, HB page 48) so it is an integral domain.

Since 11 is prime, $\mathbb{Z}_{11}$ is a field and so every non-zero element has a multiplicative inverse (Definition 1.14 of Chapter 11, R11, HB page 48).

Solution to Question 15

By Proposition 4.13 of Chapter 12 (HB page 57) a number can be expressed as the sum of two squares if, and only if, each of its prime factors of the form $4k + 3$ (if any) occurs to an even power.

In this case $5945113699 = 19^5 \times 7^4$ has two prime factors, 19 and 7.

We see that 19 is of the form $4k + 3$ and occurs to an odd power and 7 is of the form $4k + 3$ and occurs to an even power.

Therefore it is **false** that 594113699 can be expressed as the sum of two squares.

The Open University

M303

Further pure mathematics

Practice Quiz 4

Question 1

This question tests your familiarity with set notation.

Select the true statements from the following.

$\{2,4\} \subseteq (\{n \in \mathbb{N} : n \equiv 0 (\text{mod } 2)\}$
$\quad \cap \{n \in \mathbb{N} : n \leq 10\})$

$\{5\} \in \mathbb{N}$

$\{7\} \nsubseteq \{1,2,3,4,5\}$

$4 \in \{2n+1 : n \in \mathbb{N}\}$

$\{x^2 : x \in \mathbb{R}\} \subseteq \mathbb{Q}$

$a \in \{a,b,c,d,e\}$

Question 2

A [ ] (a_n) is a [ ] if, for each $\varepsilon > 0$, there is an [ ] $\in \mathbb{N}$ such that $|a_n| < \varepsilon$ whenever $n > N$.

Question 3

Find the limit as $n \to \infty$ of the sequence whose terms are $\dfrac{3 \cdot n - 5 \cdot n^4}{2 \cdot n^3 + n^2}$.

If the sequence is divergent, then enter the word "divergent" as your answer.

To determine the convergence or divergence of a real sequence, it is useful to identify the dominant terms of the numerator and denominator and compare their growth rates.

Question 4

This question is based on material in Chapter 13.

Let $f : \mathbb{R} \to \mathbb{R}$ be given by

$$f(x) = \begin{cases} 2 & \text{if } x \leq \frac{3}{2}, \\ 3 & \text{if } x > \frac{3}{2}. \end{cases}$$

Identify a point, a, at which f is discontinuous.

$a =$ [ ]

Show that f is discontinuous at a by giving an appropriate example of a real sequence (a_n) that converges to a.

$a_n =$ [ ]

Question 5

This question is based on material in Chapter 13 and can be attempted as soon as you have finished studying Chapter 13. (If you have already studied the later chapters in book D then you may assume that Euclidean metrics are used throughout the question. Please ignore the previous sentence if you have not yet studied the later chapters.)

The question asks you to decide whether the given function, $f : \mathbb{R}^2 \to \mathbb{R}$ is continuous on $\mathbb{R}^2$.

Let $f : \mathbb{R}^2 \to \mathbb{R}$ be given by

$$f(x_1, x_2) = \begin{cases} \dfrac{3x_1^2 + 4x_2}{x_1^2 \cos^2 x_2 + x_2^2} & \text{if } (x_1, x_2) \neq (0,0), \\ 0 & \text{if } (x_1, x_2) = (0,0). \end{cases}$$

Then it is [ ] that f is continuous on $\mathbb{R}^2$.

Question 6

You should be able to attempt this question after you have read Chapter 14.

This question uses a function to define a metric.

Let p be a prime number. Then for each $x \in \mathbb{Q} - \{0\}$ you may assume that there is a unique $m \in \mathbb{Z}$ so that $x = p^m \frac{a}{b}$ where $a \in \mathbb{Z} - \{0\}$ and $b \in \mathbb{Z}$ and p does not divide either a or b.

In this question we take $p = 2$ and use the above fact to define a function $f : \mathbb{Q} \to \mathbb{R}$ by:

$$f(x) = \begin{cases} 2^{-m}, & \text{if } x = 2^m \times \frac{a}{b} \text{ and 2 does} \\ & \text{not divide } a \text{ or } b \\ 0, & \text{if } x = 0 \end{cases}$$

We then define a function (that turns out to be a metric), $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ by

$$d(r, s) = f(|r - s|)$$

where $|x|$ is the absolute value of x for $x \in \mathbb{R}$.

Calculate $d(\frac{11}{3}, \frac{31}{3})$.

(See Question 9 of TMA04.)

Question 7

This question is about the sequence of functions $(f_n)_{n=1}^{\infty}$ where for $n = 1, 2, 3, \ldots$,

$f_n : [0, 1] \to \mathbb{R}$ is defined by:

$$f_n(x) = \sum_{j=1}^{n} (3 + 3^{-j} \cos jx).$$

Select the two correct statements from the following.

The n^{th} term of the sequence for $n \geq 2$, is given by: $f_n(x) = 3 + \frac{1}{3^n} \cos nx$.

The n^{th} term, $n \geq 1$, is given by: $f_n(x) = 3n + \frac{1}{3} \cos x + \cdots + \frac{1}{3^n} \cos nx$.

$f_1 = 3 + \frac{1}{3} \cos x$, $f_2(x) = 3 + \frac{1}{9} \cos 2x$.

$f_1(x) = 3 + \frac{1}{3} \cos x$, $f_2(x) = 6 + \frac{1}{3} \cos x + \frac{1}{9} \cos 2x$.

Question 8

This question assesses your understanding of the definition of a metric.

Let X be any set and let $\mathcal{F}(X)$ be the set of finite subsets of X. If A and B are elements of $\mathcal{F}(X)$ we define a distance function $d : \mathcal{F}(X) \times \mathcal{F}(X) \to \mathbb{R}$ by

$$d(A, B) = |(A \cup B) - (A \cap B)|,$$

where $|A|$ denotes the number of elements in A.

Determine whether the following statement is *True* or *False*:

The distance function d is always a metric for $\mathcal{F}(X)$.

(*Hint*: use Venn diagrams to check M3.)

Select one:

True

False

Question 9

This question is based on material in Chapter 14.

Consider the following subsets of $\mathbb{R}^2$ where $d^{(2)}$ is the Euclidean metric, d_0 is the discrete metric and d is the taxicab metric.

Let $A = B_{d_0}((0, 0), \frac{1}{2})$. Let $B = B_{d_0}((0, 0), 1)$.

Let $C = B_{d_0}[(0, 0), 1]$. Let $D = B_d[(0, 0), 1]$.

Let $E = B_{d^{(2)}}((0, 0), 1)$.

In the following four statements, determine which of the phrases 'is contained in', 'contains', 'is equal to', 'is neither contained

in, nor contains' should be in the blank spaces.

The set A [ ] the set B.

The set C [ ] the set D.

The set D [ ] the set E.

The set E [ ] the set A.

Question 10

This question is based on material in Chapter 14.

Let (X, d) and (Y, e) be two metric spaces, with $A \subseteq X$ and let $f : A \to Y$ be a function from A to Y.

Which of the following is written correctly:

f is (e, d_A)-continuous at $f(x) \in f(A)$ if: whenever $(f(x_k))$ is an e-convergent sequence with $f(x_k) \to f(x)$ as $k \to \infty$ in $f(A)$, then the sequence (x_k) is d_A-convergent to x.

f is (e, d)-continuous at $f(x) \in Y$ if: whenever $(f(x_k))$ is an e-convergent sequence with $f(x_k) \to f(x)$ as $k \to \infty$ in Y, then the sequence (x_k) is d-convergent to x.

f is (d, e)-continuous at $x \in X$ if: whenever (x_k) is a d-convergent sequence with $x_k \to x$ as $k \to \infty$ in X, then the sequence $(f(x_k))$ is e-convergent to $f(x)$.

f is (d_A, e)-continuous at $x \in A$ if: whenever (x_k) is a d_A-convergent sequence with $x_k \to x$ as $k \to \infty$ in A, then the sequence $(f(x_k))$ is e-convergent to $f(x)$.

f is (d_A, e)-continuous at $x \in A$ if: whenever (x_k) is a d_A-convergent sequence with $x_k \to x$ as $k \to \infty$ in A, then the sequence $(f(x_k))$ is also d-convergent to $f(x)$.

f is (d_A, e)-continuous at $x \in X$ if: whenever (x_k) is a d_A-convergent sequence with $x_k \to x$ as $k \to \infty$ in X, then the sequence $(f(x_k))$ is e-convergent to $f(x)$.

Question 11

This question is based on material in Chapters 14 and 15.

The following statements all concern the sequence $\left(\frac{1}{n}\right)_{n\in\mathbb{N}}$ but for different choices of metric space (X, d).

Determine whether the sequence converges or diverges for the particular choice of metric space.

If $X = (0, \infty)$ and $d = d_0$, then $\left(\frac{1}{n}\right)$ [ ].

If $X = [0, \infty)$ and $d = d_0$, then $\left(\frac{1}{n}\right)$ [ ].

If $X = (0, \infty)$ and $d = d^{(1)}_{(0,\infty)}$, then $\left(\frac{1}{n}\right)$ [ ].

If $X = \mathbb{Q}$ and $d = d^{(1)}_{\mathbb{Q}}$, then $\left(\frac{1}{n}\right)$ [ ].

Question 12

You should be able to do this question after reading Chapters 14 and 15.

Let a metric $d : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ be defined by:

$d((x_1, y_1), (x_2, y_2)) = d_0(x_1, x_2) + d^{(1)}(y_1, y_2)$, where d_0 is the discrete metric on $\mathbb{R}$ and $d^{(1)}$ is the Euclidean metric on $\mathbb{R}$.

Which one of the following sets corresponds to $B_d[(1, 2), 1]$?

$\{(x, 2) \in \mathbb{R}^2 : x \in \mathbb{R}\} \cup \{(1, y) \in \mathbb{R}^2 : 1 \leq y \leq 3\}$

$\{(1, y) \in \mathbb{R}^2 : 1 \leq y \leq 3\}$

$\{(x, 2) \in \mathbb{R}^2 : 0 \leq x \leq 2\}$

$\{(x, y) \in \mathbb{R}^2 : 0 < x < 2 \text{ and } 1 \leq y \leq 3\}$

$\{(1, y) \in \mathbb{R}^2 : y \in \mathbb{R}\} \cup \{(x, 2) \in \mathbb{R}^2 : 0 < x < 2\}$

$\{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } 1 < y < 3\}$

Question 13

You should be able to do this question after reading Chapters 14 and 15.

Let a metric $d : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ be defined by:

$d((x_1, y_1), (x_2, y_2)) =$
$\max\{d^{(1)}(x_1, x_2), d_0(y_1, y_2)\}$, where d_0 is the discrete metric on $\mathbb{R}$ and $d^{(1)}$ is the Euclidean metric on $\mathbb{R}$.

Which one of the following sets corresponds to $B_d((1, 3), 2)$?

$\{(x, y) \in \mathbb{R}^2 : -1 < x < 3\}$

$\{(1, 3)\}$

$\{(x, y) \in \mathbb{R}^2 : -1 < x < 3 \text{ and } 1 < y < 5\}$

$\{(1, y) \in \mathbb{R}^2 : 1 \leq y \leq 5\}$

$\{(x, 3) \in \mathbb{R}^2 : -1 < x < 3\}$

$\{(x, y) \in \mathbb{R}^2 : -1 < x < 3 \text{ and } 1 \leq y \leq 5\}$

Question 14

You should be able to do this question after reading Chapters 14 and 15.

Let a metric $d : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ be defined by:

$d((x_1, y_1), (x_2, y_2)) =$
$\max\{d^{(1)}(x_1, x_2), d_0(y_1, y_2)\}$, where d_0 is the discrete metric on $\mathbb{R}$ and $d^{(1)}$ is the Euclidean metric on $\mathbb{R}$.

Which one of the following sets corresponds to $S_d((1, 3), 1)$?

$\{(x, y) \in \mathbb{R}^2 : y \neq 3\}$

$\{(0, 3), (2, 3)\}$

$\{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } y \neq 3\} \cup \{(0, 3), (2, 3)\}$

$\{(x, y) \in \mathbb{R}^2 : 0 < x < 2 \text{ and } y \neq 3\} \cup \{(0, 3), (2, 3)\}$

$\{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } y \neq 3\}$

$\{(x, y) \in \mathbb{R}^2 : 0 < x < 2 \text{ or } y \neq 3\}$

Question 15

This question is based on material in Chapter 16.

Suppose that d is the Euclidean metric for $\mathbb{R}$ and $A = (0, 2] \cup [3, 5)$. Let d_A be the induced metric for A.

Define $C = [1, 5) \cap A$.

Select the true statements from the following:

C is d-open in $\mathbb{R}$.

C is d_A-open in A.

C is d_A-closed in A.

C is neither d-open nor d-closed in $\mathbb{R}$.

$C = [1, 2) \cup [3, 5)$.

C is d-closed in $\mathbb{R}$.

$C = [1, 2] \cup [3, 5)$.

C is neither d_A-open nor d_A-closed in A.

Question 16

This question is based on material in Chapter 16.

Let d denote the Euclidean metric, $d^{(1)}$, for $\mathbb{R}$. This question asks you to decide whether certain subsets of $\mathbb{R}$ are d-closed, d-open, both d-closed and d-open or neither d-closed nor d-open when considered as subsets of $\mathbb{R}$.

Determine which of the phrases 'd-closed but not d-open', 'd-open but not d-closed', 'd-closed and d-open', and 'not d-closed and not d-open' should appear in the blank spaces below.

1. The subset $(1, 2) \cup (2, 3)$ is [ ] when considered as a subset of $(\mathbb{R}, d)$.
2. The subset $\{p \in \mathbb{N} : p \text{ is prime}\}$ is [ ] when considered as a subset of $(\mathbb{R}, d)$.

Question 17

This question is based on material in Chapter 16.

Let $A = \{(x, y) \in \mathbb{R}^2 : x < 0\}$ and $B = \{(x, y) \in \mathbb{R}^2 : -2 < x < 2$ and $-2 \leq y \leq 2\}$.

Define $C = A \cap B$.

For the Euclidean metric d on the plane, select the correct options from the following:

Select one or more:

$\mathrm{Cl}_d(C) = \{(x, y) \in \mathbb{R}^2 : 0 \leq x \leq 2$ and $-2 \leq y \leq 2\}$

$\mathrm{Cl}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 \leq x \leq 0$ and $-2 \leq y \leq 2\}$

$C = \{(x, y) \in \mathbb{R}^2 : 0 < x < 2$ and $-2 \leq y \leq 2\}$

$\mathrm{Cl}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 < x < 0$ and $-2 < y < 2\}$

$\mathrm{Int}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 \leq x \leq 0$ and $-2 \leq y \leq 2\}$

$\mathrm{Int}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 < x < 0$ and $-2 < y < 2\}$

$C = \{(x, y) \in \mathbb{R}^2 : -2 < x < 0$ and $-2 \leq y \leq 2\}$

Question 18

This question is based on material in Chapter 16.

Select any of the following statements that are true.

There is a rational number lying between any two non-equal irrational numbers in the interval $(0, 1)$.

There is an irrational number lying between any two non-equal rational numbers in the interval $(0, 1)$.

There is a one-one map between the set of all rational numbers lying in the interval $(0, 1)$ and the set of all irrational numbers lying in the interval $(0, 1)$.

Solutions

Solution to Question 1

The correct answers are:

$a \in \{a, b, c, d, e\}$.

$\{2, 4\} \subseteq (\{n \in \mathbb{N} : n \equiv 0 (\text{mod } 2)\} \cap \{n \in \mathbb{N} : n \leq 10\})$. This is correct since $\{n \in \mathbb{N} : n \equiv 0 (\text{mod } 2)\} \cap \{n \in \mathbb{N} : n \leq 10\} = \{2, 4, 6, 8, 10\}$. Hence $\{2, 4\}$ is a subset of $\{n \in \mathbb{N} : n \equiv 0 (\text{mod } 2)\} \cap \{n \in \mathbb{N} : n \leq 10\}$.

$\{7\} \nsubseteq \{1, 2, 3, 4, 5\}$.

Page 6 of the Handbook summarises the basic set notation that we expect you to be already familiar with and page 7 lists some standard sets.

Remember: $\in$ means 'is an element of', $\subseteq$ means 'is a subset of', $\cap$ denotes set intersection, $\cup$ denotes set union and ϕ denotes the empty set.

Solution to Question 2

The correct answer is: A [real sequence] (a_n) is a [null sequence] if, for each $\varepsilon > 0$, there is an $[N] \in \mathbb{N}$ such that $|a_n| < \varepsilon$ whenever $n > N$.

You should have given the definition of a null sequence:

See Definition 1.10 of Chapter 13 (page 63 of the Handbook) to remind yourself of the definition of a real null sequence. They are a basic tool in the study of metric spaces and you *really* should learn the definition.

Solution to Question 3

A correct answer is: the sequence diverges to $-\infty$.

Solution to Question 4

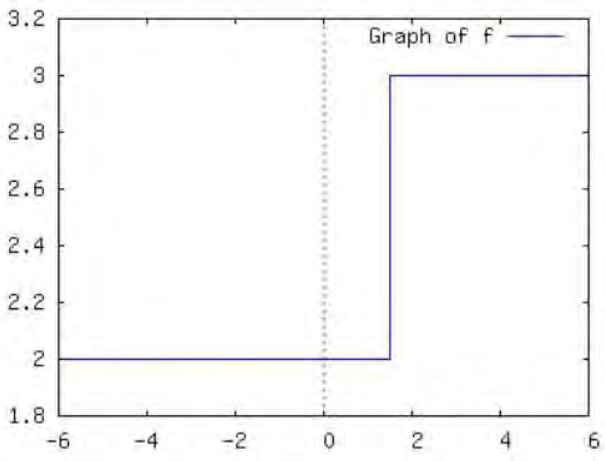
A correct answer is $\frac{3}{2}$, which can be typed in as follows: 3/2

A correct answer is $\frac{3}{2} - \frac{1}{n}$, which can be typed in as follows: 3/2 − 1/n.

Worked solution

To show that a function f has a discontinuity at a point a, it is enough to find a sequence (a_n) for which $\lim_{n\to\infty} a_n = a$ and yet the sequence $(f(a_n))$ does not converge to $f(a)$.

If we plot the graph for the function f in this question (ignore the vertical line - it is an artefact), we obtain



and the discontinuity appears to be at $a = \frac{3}{2}$.

If we take a sequence whose terms are given by $a_n = \frac{1}{n} + \frac{3}{2}$ for $n \in \mathbb{N}$, then $a_n \to \frac{3}{2}$ as $n \to \infty$ and yet

$$f(a_n) \to 3 \neq f\left(\tfrac{3}{2}\right) = 2.$$

Hence f is discontinuous at $\frac{3}{2}$.

Solution to Question 5

(See Worked Exercise 3.12 and Exercise 3.4 of Chapter 13, pages 44 and 45 for related examples.)

It is false that

$f : \mathbb{R}^2 \to \mathbb{R}$ given by

$$f(x_1, x_2) = \begin{cases} \dfrac{3x_1^2 + 4x_2}{x_1^2 \cos^2 x_2 + x_2^2} & \text{if } (x_1, x_2) \neq (0,0), \\ 0 & \text{if } (x_1, x_2) = (0,0). \end{cases}$$

is continuous on $\mathbb{R}^2$. There is more than way to show this and the method below is just one possible approach.

The function is made up of sums, multiples and products of powers of the projection functions p_1 and p_2 (Definition 3.10 of Chapter 13, HB page 68) together with a composition of a trigonometric function with a projection function p_2, all of which are continuous. Hence use of the composition rule (Proposition 3.16, HB page 68) together with the combination rules for continuous functions from $\mathbb{R}^2$ to $\mathbb{R}$ tell us that sums, products and multiples of these are continuous (HB page 68) and that quotients, f/g are continuous provided $g(x) \neq 0$. So the only place that there can be a problem is at the origin.

By Definitions 3.8 and 3.9 of Chapter 13 (HB pages 67 and 68), f is a continuous function from $\mathbb{R}^2$ to $\mathbb{R}$ if whenever $(\mathbf{x_n})$ is a sequence in $\mathbb{R}^2$ converging to $\mathbf{a}$ (for any point $\mathbf{a} \in \mathbb{R}^2$), then the real sequence $(f(\mathbf{x_n}))$ converges to $f(\mathbf{a}) \in \mathbb{R}$. Therefore to show that f is discontinuous at the point x, we just need to find one sequence $(\mathbf{x_n})$ in $\mathbb{R}$ with $(\mathbf{x_n}) \to \mathbf{x}$ and the sequence $(f(\mathbf{x_n}))$ not converging to $f(\mathbf{x})$.

Therefore it seems sensible to try looking at what happens if we take a sequence that tends to $(0,0)$.

There are lots of different sequences that converge to $(0,0)$ that we could choose here. We want to keep things as simple as possible so we consider the sequence $\left(\left(\frac{1}{n}, 0\right)\right)$, since taking $x_2 = 0$ removes the $\cos^2 x_2$ term (since $\cos 0 = 1$), as well as removing the other x_2 terms.

We have:
$d^{(2)}\left(\left(\frac{1}{n}, 0\right), (0,0)\right) = \frac{1}{n} \to 0$ as $n \to \infty$ and so our sequence does tend to $(0,0)$ in $\mathbb{R}^2$.

However $f\left(\frac{1}{n}, 0\right) = \dfrac{3\frac{1}{n^2} + 0}{\frac{1}{n^2} + 0} = 3$ for each $n \in \mathbb{N}$ and so $f\left(\left(\frac{1}{n}, 0\right)\right)$ is the constant sequence where every term is 3 which clearly does not converge to $f(0,0) = 0$.

Therefore f is not continuous at $(0,0)$ and hence is not continuous on $\mathbb{R}^2$.

Solution to Question 6

A correct answer is $\frac{1}{4}$, which can be typed in as follows: 1/4.

The answer (as a fraction in its lowest terms) is $\frac{1}{4}$.

We proceed as follows.

First we note that $d(r,s) = f(r-s)$ and so

$$d(\tfrac{11}{3}, \tfrac{31}{3}) = f(|\tfrac{11}{3} - \tfrac{31}{3}|).$$

We have:

$$\begin{aligned} |\tfrac{11}{3} - \tfrac{31}{3}| &= \tfrac{31-11}{3} \\ &= \tfrac{20}{3} \end{aligned}$$

Therefore we need to calculate $f(\frac{20}{3})$.

In order to do this we need to write $\frac{20}{3}$ in the form $2^m \times \frac{a}{b}$ where 2 does not divide a or b.

Since $\text{hcf}(2,3) = 1$, and $20 = 2^2 \times 5$ (with $\text{hcf}(2,5) = 1$), we see that the required form is:

$$\tfrac{20}{3} = 2^2 \times \tfrac{5}{3}.$$

Therefore

$$\begin{aligned} d(\tfrac{11}{3}, \tfrac{31}{3}) &= f(\tfrac{20}{3}) \\ &= f(2^2 \times \tfrac{5}{3}) \\ &= 2^{-2} \\ &= \tfrac{1}{4} \end{aligned}$$

Solution to Question 7

The correct answers are:

$f_1(x) = 3 + \frac{1}{3}\cos x$, $f_2(x) = 6 + \frac{1}{3}\cos x + \frac{1}{9}\cos 2x$., The n^{th} term, $n \geq 1$, is given by: $f_n(x) = 3n + \frac{1}{3}\cos x + \cdots + \frac{1}{3^n}\cos nx$.

Sequences of functions are discussed in Sections 4 and 5 of Chapter 15 (pages 78, 79 and 80 of the Handbook).

Solution to Question 8

The correct answer is 'True'.

This is a metric (see Definition 2.1 of Chapter 14 on page 72 of the handbook).

(M1) $(A \cup A) = (A \cap A) = A$ and so $d(A, A) = |\phi| = 0$.

(M2) $A \cup B = B \cup A$ and $A \cap B = B \cap A$ and so $d(A, B) = d(B, A)$.

(M3) This can be seen by drawing a Venn diagram and by noting that any points that are in $A \cup C$ but not in $A \cap C$ occur in at least one of $(A \cup B) - (A \cap B)$ and $(B \cup C) - (B \cap C)$.

Solution to Question 9

The correct answer is

The set A [is equal to] the set B.

The set C [contains] the set D.

The set D [is neither contained in, nor contains] the set E.

The set E [contains] the set A.

The Euclidean metric for the plane is defined in Definition 3.3 of Chapter 13 (HB page 67).

The discrete metric is defined in Definition 2.3 of Chapter 14 (HB page 72).

The taxicab metric for the plane is defined on page 91 of Book D in Chapter 14, Section 2 (HB page 61).

Calculation shows that:

$A = B_{d_0}((0,0), \frac{1}{2}) = \{(0,0)\}$, the set containing only the point $(0,0)$.

$B = B_{d_0}((0,0), 1) = \{(x_1, x_2) \in \mathbb{R}^2 : d_0((0,0),(x_1,x_2)) < 1\} = \{(0,0)\}$, the set containing only the point $(0,0)$.

$C = B_{d_0}[(0,0), 1] = \{(x_1, x_2) \in \mathbb{R}^2 : d_0((0,0),(x_1,x_2)) \leq 1\} = \mathbb{R}^2$.

D is similar to the diamond illustrated on page 96 of Chapter 14 but includes the boundary, and

E is the usual open unit ball centred on the origin.

Hence

$$A = B \subseteq D$$

and $E \subseteq C$. However $D \nsubseteq E$ and $E \nsubseteq D$.

Solution to Question 10

The correct answer is: f is (d_A, e)-continuous at $x \in A$ if:
whenever (x_k) is a d_A-convergent sequence with $x_k \to x$ as $k \to \infty$ in A, then the sequence $(f(x_k))$ is e-convergent to $f(x)$.

The definition of continuity at a point for a function between two metric spaces is given in Definition 4.1 of Chapter 14 (HB page 73).

We also need to be careful to work with the induced metric on the domain of the function, e_A - see Definition 1.4 of Chapter 15 (HB page 74).

Solution to Question 11

The correct answers are:

If $X = (0, \infty)$ and $d = d_0$, then $\left(\frac{1}{n}\right)$ [diverges].

If $X = [0, \infty)$ and $d = d_0$, then $\left(\frac{1}{n}\right)$ [diverges].

If $X = (0, \infty)$ and $d = d^{(1)}_{(0,\infty)}$, then $\left(\frac{1}{n}\right)$ [diverges].

If $X = \mathbb{Q}$ and $d = d^{(1)}_{\mathbb{Q}}$, then $\left(\frac{1}{n}\right)$ [converges].

The definition of convergence for a sequence in a metric space is given in Definition 3.2 of Chapter 14 (HB page 73).

The only convergent sequences for (X, d_0), regardless of the choice of X are the eventually constant sequences (see Exercise 3.2 of Chapter 14) and so the

sequence $\left(\frac{1}{n}\right)$ is divergent in (X, d_0) for any valid choice of X.

For the latter two spaces, we note that the metric in each case is the induced metric from the Euclidean metric for $\mathbb{R}$ (see Definition 1.4 of Chapter 15).

For $X = (0, \infty)$, we note that the sequence $\left(\frac{1}{n}\right)$ is divergent, since the only possible limit is 0 and this is not in X. (See Theorem 1.5 of Chapter 15, HB page 74.)

For $\mathbb{Q}$, we note that each term of the sequence $\left(\frac{1}{n}\right)$ is in $\mathbb{Q}$ as is the possible limit 0. Moreoever, since $\left(\frac{1}{n}\right)$ is a basic null sequence, we deduce from Theorem 1.5 of Chapter 15 (HB page 74) that $\left(\frac{1}{n}\right)$ is $d_{\mathbb{Q}}^{(1)}$-convergent to 0.

Solution to Question 12

By Definition 2.6 of Chapter 14(HB page 72),

$$B_d[(1,2),1] = \{(x,y) \in \mathbb{R} : d_0(x,1) + |y-2| \leq 1\}.$$

The metric d is a product metric. Product metrics are covered in Section 1.3 of Chapter 15.

First we consider any points in the set $\{(x,y) \in \mathbb{R}^2 : x \neq 1\}$. For these points we have $d_0(x,1) = 1$, so

$$\begin{aligned} d((x,y),(1,2)) &= d_0(x,1) + |y-2| \\ &= 1 + |y-2|. \end{aligned}$$

This will be less than or equal to 1 if, and only if, $|y-2| = 0$ meaning that $y = 2$. Therefore all points of the form $(x,2), x \neq 1$, will be in $B_d[(1,2),1]$.

Now we consider points of the form $(1,y)$.

$$\begin{aligned} \text{Here } d((1,y),(1,2)) &= d_0(1,1) + |y-2| \\ &= 0 + |y-2| \\ &= |y-2|. \end{aligned}$$

This will be less than or equal to 1 if, and only if, $1 \leq y \leq 3$.

Therefore $B_d[(1,2),1] = \{(x,2) \in \mathbb{R}^2 : x \in \mathbb{R}\} \cup \{(1,y) \in \mathbb{R}^2 : 1 \leq y \leq 3\}$.

Solution to Question 13

The correct answer is $\{(x,y) \in \mathbb{R}^2 : -1 < x < 3\}$.

By Definition 2.6 of Chapter 14 (HB page 72), $B_d((1,3),2) = \{(x,y) \in \mathbb{R}^2 : \max\{|x-1|, d_0(y,3)\} < 2\}$.

By definition of d_0 (Definition 2.3 of Chapter 14, HB page 72), we know that $d_0(a,b) < 2$ for any a and b. Therefore $\max\{|x-1|, d_0(y,3)\}$ can only be greater than or equal to 2 if $|x-1| \geq 2$.

Therefore $\max\{|x-1|, d_0(y,3)\} < 2$ if, and only if $|x-1| < 2$, that is if, and only if, $-1 < x < 3$.

Therefore $B_d((1,3),2) = \{(x,y) \in \mathbb{R}^2 : -1 < x < 3\}$.

Solution to Question 14

The correct answer is $\{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } y \neq 3\} \cup \{(0,3),(2,3)\}$.

By Definition 2.6 of Chapter 14 (HB page 72), $S_d((1,3),1) = \{(x,y) \in \mathbb{R}^2 : \max\{|x-1|, d_0(y,3)\} = 1\}$.

A point (x,y) will be in $S_d((1,3),1)$ if, and only if $\max\{|x-1|, d_0(y,3)\} = 1$. This will happen if one (or both) of the following holds:

case 1:$|x-1| = 1$ and $d_0(y,3) \leq 1$ or

case 2:$|x-1| \leq 1$ and $d_0(y,3) = 1$

We consider each case in turn.

Case 1

By definition $d_0(y,3)$ is always less than or equal to 1 (Definition 2.3 of Chapter 14, HB page 72). Therefore case 1 will hold if, and only if, $|x-1| = 1$, that is if, and only if, $x = 0$ or $x = 2$.

Therefore

$$\{(0,y) \in \mathbb{R}^2 : y \in \mathbb{R}\} \cup \{(2,y) \in \mathbb{R}^2 : y \in \mathbb{R}\} \subseteq S_d((1,3),1).$$

Note that this set corresponds to two vertical lines in $\mathbb{R}^2$, one through the point $(0,0)$ and one through the point $(2,0)$.

Case 2

Again by definition $d_0(y,3) = 1$ for any $y \neq 3$. Therefore $|x-1| \leq 1$ and $d_0(y,3) = 1$ if, and only if $|x-1| \leq 1$ and $y \neq 3$.

Therefore

$$\{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } y \neq 3\} \subseteq S_d((1,3),1).$$

Note that this set is the 'vertical strip' of $\mathbb{R}^2$ corresponding to $0 \leq x \leq 2$ with the horizontal line segment corresponding to $y = 2$ missing. Note also that the only points satisfying Case 1 that do not lie in this set are the two points $(0,3)$ and $(2,3)$.

Putting these together we see that:

$$S_d((1,3),1) = \{(x,y) \in \mathbb{R}^2 : 0 \leq x \leq 2 \text{ and } y \neq 3\} \cup \{(0,3),(2,3)\}$$

Solution to Question 15

The correct answers are: C is neither d-open nor d-closed in $\mathbb{R}$, $C = [1,2] \cup [3,5)$, C is d_A-closed in A.

We find that

$$\begin{aligned} C &= [1,5) \cap A \\ &= [1,5) \cap ((0,2] \cup [3,5)) \\ &= ([1,5) \cap (0,2]) \cup ([1,5) \cap [3,5)) \\ &= [1,2] \cup [3,5). \end{aligned}$$

Since C can be written as the intersection of a d-closed subset of $\mathbb{R}$ with A (for example, $C = [1,6] \cap A$), we can use Theorem 3.12 of Chapter 16 (HB page 84) to conclude that C is d_A-closed.

Since $C = [1,2] \cup [3,5)$, C is not d-closed. (Consider the sequence $(5 - \frac{1}{n})_{n \in \mathbb{N}}$.) By considering open balls around the points 1, 2 or 3, we see that C is not d-open.

The complement of C in A is

$$\begin{aligned} A - C &= ((0,2] \cup [3,5)) - ([1,2] \cup [3,5)) \\ &= (0,1) \end{aligned}$$

and this set cannot be written as the intersection of a d-closed set with A and so is not d_A-closed.

Hence C is not d_A-open.

Solution to Question 16

The correct answer is

1. The subset $(1,2) \cup (2,3)$ is [d-open but not d-closed] when considered as a subset of $(\mathbb{R}, d)$.
2. The subset $\{p \in \mathbb{N} : p \text{ is prime}\}$ is [d-closed but not d-open] when considered as a subset of $(\mathbb{R}, d)$.

Note that the solutions given below are not the only ways of answering this question and there are many other possible approaches.

A strategy to determine whether sets are open or closed can be found on page 83 of the Handbook and a table containing examples of open and closed sets can be found on page 89 of the Handbook.

1. The subset $(1,2) \cup (2,3)$ is d-open but not d-closed when considered as a subset of $(\mathbb{R}, d)$. To see this we argue as follows:

   The open intervals (1,2) and (2,3) are both d-open by the table in the handbook (HB page 89).

   Therefore $(1,2) \cup (2,3)$ is also d-open by Theorem 2.15 of Chapter 16 (HB page 82).

   The subset $(1,2) \cup (2,3)$ is not d-closed. To see this note that the point 1 is not an element of $(1,2) \cup (2,3)$ but is the d-limit of the sequence $(1 + \frac{1}{n+1})_{n \in \mathbb{N}}$ and this sequence lies within $(1,2) \cup (2,3)$. Therefore this set is not d-closed by Definition 1.1 of Chapter 16 (HB page 80).
2. $\{p \in \mathbb{N} : p \text{ is prime}\}$ is d-closed and not d-open. To see that it is d-closed we consider the complement $C = \mathbb{R} - \{p \in \mathbb{N} : p \text{ is prime}\}$ and show that this is d-open. We do this by showing that for any $c \in C$ we can find an r with $B_d(c,r) \subseteq C$. Let $c \in C$. To simplify the language we consider the cases $c < 2$ and $c > 2$ separately.

First assume $c < 2$. Let $r = \frac{(2-c)}{2}$. Then, by inspection, $B_d(c, r) \subseteq C$.

Now assume that $c > 2$. Then c must lie between two adjacent primes p and q. Let $r = \min\{\frac{|p-c|}{2}, \frac{|q-c|}{2}\}$. Then, by inspection, $B_d(c, r) \subseteq C$. Therefore by Theorem 2.9 of Chapter 16 (HB page 82) C is d-open and so by Definition 2.1 of Chapter 16 (HB [page 81) $\{p \in \mathbb{N} : p \text{ is prime}\}$ is d-closed.

To see that it is not d-open we note that any d-open ball around the point $2 \in \{p \in \mathbb{N} : p \text{ is prime}\}$ contains the point $2 + s$ where $s = \min\{\frac{r}{2}, \frac{1}{2}\}$ and that this point is not in $\{p \in \mathbb{N} : p \text{ is prime}\}$. Therefore by Theorem 2.9 the set is not d-open.

Solution to Question 17

The correct answer is
$\mathrm{Cl}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 \leq x \leq 0$
and $-2 \leq y \leq 2\}$,
$\mathrm{Int}_d(C) = \{(x, y) \in \mathbb{R}^2 : -2 < x < 0$
and $-2 < y < 2\}$,
$C = \{(x, y) \in \mathbb{R}^2 : -2 < x < 0$
and $-2 \leq y \leq 2\}$.

When given questions like this, it is often helpful to sketch the sets to help ensure that you don't make silly errors.

We calculate that

$$\begin{aligned} C &= A \cap B \\ &= \{(x, y) \in \mathbb{R}^2 : x < 0\} \cap \{(x, y) \in \mathbb{R}^2 : -2 < x < 2 \\ &\quad \text{and } -2 \leq y \leq 2\} \\ &= \{(x, y) \in \mathbb{R}^2 : -2 < x < 0 \text{ and } -2 \leq y \leq 2\} \end{aligned}$$

from which we can read off the closure and interior for the Euclidean metric.

Solution to Question 18

The correct answer is: There is a rational number lying between any two non-equal irrational numbers in the interval $(0, 1)$., There is an irrational number lying between any two non-equal rational numbers in the interval $(0, 1)$.

See the 'density property of the reals' (HB page 7), Chapter 16 section 6, and the table on page 87 of the handbook.

The Open University

M303

Further pure mathematics

Practice Quiz 5

Question 1

This question revises some material from Book C that will be used in Book E. You can attempt this question before you start reading Book E.

Complete the following statement to make it correct.

It is ☐ that $\mathbb{Z}_{11}$ is an integral domain.

Question 2

This question revises some material from Book C that will be used in Book E. You can attempt this question before you start reading Book E.

Let R be a commutative ring. We say that a non-zero element $x \in R$ is ☐ if whenever x divides a product, $yz \in R$, with $y, z \in R$ then x divides one of y or z.

Let R be a commutative ring. We say that a non-zero element $x \in R$ is ☐ if it is not a unit and if we cannot write x as a product, $x = yz$, with $y, z \in R$ unless one of y or z is a unit.

Let R be a commutative ring. If a non-zero element $x \in R$ has a multiplicative inverse then we say that x is ☐.

Let R be a commutative ring. If $x = u \times y$ where u is a unit then we say that x is ☐ of y.

Question 3

This question revises some material from Book C that will be used in Book E. You can attempt this question before you start reading Book E.

Let R be a ring. Which of the following statements are always true if R is a Euclidean domain?

If $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$.

There exists a function $N : R\{0\} \to \mathbb{N} \cup \{0\}$ such that for non-zero $a, b \in R$ we have $N(a) \leq N(ab)$ and there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

Every non-zero non-unit element of R can be written as a product of irreducibles and this product is unique up to associates.

R is closed under addition and multiplication, addition is commutative and R has an additive identity. In other words for all a and b in R, we have $a + b, a \times b \in R; a + b = b + a$ and there is an element $0 \in R$ with $a + 0 = a$.

The multiplicative identity, 1, of R, is not equal to the additive identity, 0, and all elements of R have a multiplicative inverse. In other words for all $r \in R$ we can find an element $s \in R$ with $r \times s = s \times r = 1$.

Question 4

You should be able to attempt this question after reading Chapter 17.

Write the appropriate expressions in the empty boxes.

Every ☐ is a ☐. (Euclidean Domain, Field)

Every [ ] is a [ ]. (Principle Ideal Domain, Unique Factorisation Domain)

All [ ] are also [ ]. (Commutative rings, Integral Domains)

Question 5

You should be able to do this question after reading Chapter 17.

In which of the following is the set A an ideal of the ring R? (In each case you may assume that R is a ring.)

Let R be the ring $\mathbb{Z}$ with the usual operations of $+$ and $\times$ and let $A = \{2^n \in \mathbb{Z} : n \in \mathbb{N}\}$.

Let $R = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with addition and multiplication modulo 8 and let $A = \{0, 4\}$.

Let R be the ring of Gaussian integers $\mathbb{Z}[i]$ with the usual operations of $+$ and $\times$ and let $A = \{2m_1 + 2m_2 i : m_1, m_2 \in \mathbb{Z}\}$.

Let $R = \mathbb{Q}[x]$ and $A = \{\text{polynomials } p(x) \text{ in } \mathbb{Q}[x] \text{ with } p(4) = 0\}$.

Let $R = \mathbb{Z}$ with the usual addition and multiplication, and let $A = \{\pm p : p \text{ is prime}\} \cup \{0\}$.

Question 6

You should be able to do this question after reading Chapter 17.

In the ring $\mathbb{Z}$ what is the value of a for which $\langle a \rangle = \langle 2 \rangle + \langle 10 \rangle$?

Question 7

You should be able to do this question after reading Chapter 17.

Let $M_2 \left\{ \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} : z_1, z_2 \in \mathbb{Z} \right\}$ be the ring of 2×2 diagonal matrices with integer entries (you may assume that this is a commutative ring with a 1) and $f : M_2 \to \mathbb{Z}$ be the ring homomorphism given by $\begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} \mapsto z_1$. You may assume that this is a ring homomorphism.

Which of the following are true?

The kernel of f is equal to $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & z \end{pmatrix} : z \in \mathbb{Z} \right\} \subseteq M_2$ and is a subgroup of the additive group of M_2

The kernel of f is equal to $\{0\} \subseteq \mathbb{Z}$ and is a subgroup of the additive group of $\mathbb{Z}$.

The map f is one-one

The map f is onto

The image of f is given by $\mathrm{Im}(f) = \left\{ \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} : z \in \mathbb{Z} \right\} \subseteq M_2$

The image of f is given by $\mathrm{Im}(f) = \mathbb{Z}$.

Question 8

You should be able to do this question after reading Chapter 17.

Select all of the following algebraic objects in which every non-zero non-unit element a is expressible as a product of irreducibles, $a = p_1 \dots p_n$, and which is such that if $a = p_1 \dots p_n$ and $a = q_1 \dots q_m$, then $n = m$ and the p_i and q_j pair off as associates.

A group

An integral domain

A field

A unique factorisation domain

A ring

A principal ideal domain

A Euclidean domain

Question 9

You should be able to do this question after reading Chapter 17.

Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ and } i^2 = -1\}$ be the ring of Gaussian integers and recall that it is a Euclidean domain when given the norm $N(a + bi) = a^2 + b^2$.

Select the highest common factor(s) of $5 - 8i$ and $7 + 3i$ from the following list.

$-2 + i$

1

i

$-i$

$2 - i$

$-1 - 2i$

Question 10

You should be able to do this question after reading Chapter 17. It also revises some material from Book C.

Which of the following statements are always true. Select all that apply.

In a ring maximal ideals are prime

In a principal ideal domain non-trivial prime ideals are maximal

In a unique factorisation domain all irreducibles are prime

In an integral domain all primes are irreducible

In an integral domain all irreducibles are prime

In a unique factorisation domain all primes are irreducible.

Question 11

You should be able to do this question after reading Chapter 18.

How many primitive elements are there in the field of order 27?

Question 12

You should be able to do this question after reading Chapter 18.

Show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{5})$ and hence determine $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}]$. (You may assume that $\sqrt{5}$ and $\sqrt{3}$ are irrational.)

The degree of $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}]$ is

[ ].

Question 13

You should be able to do this question after reading Chapter 18.

The polynomial $x^2 - x + 1$ is irreducible over $\mathbb{Z}_5[x]$ and so $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$ is a field (Proposition 1.5 of Chapter 18, HB page 100). This means that any element of $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$ has a multiplicative inverse.

Find the multiplicative inverse of $3x + 2$ in $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$.

The multiplicative inverse of $3x + 2$ in the field $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$ is

[ ].

Question 14

You should be able to do this question after reading Chapter 18.

Let $f(x)$ be a polynomial in the ring $R = \mathbb{Z}[x]$ and let $f'(x)$ be its formal derivative, that is:

if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then
$f'(x) = na_n x^{n-1} + (n-1)a_{n_1}x^{n-2} + \cdots + a_1$.

Which of the following subsets of R are an ideal in R?

$\{f(x) \in R : f(2) = f'(2) = 0\}$

$\{f(x) \in R : f'(2) = 0\}$

$\{f(x) \in R : f(2) + f'(2) = 0\}$

$\{f(x) \in R : f(2) = f(5) = 0\}$

Question 15

You should be able to do this question after reading Chapter 18.

Consider $\mathbb{Z}_7[x]$. Which of the following statements are true?

$\mathbb{Z}_7[x]$ is a UFD.

$\mathbb{Z}_7[x]$ is a field.

$\mathbb{Z}_7[x]$ is a Euclidean Domain.

$\mathbb{Z}_7[x]$ is finite.

$x^2 + 1$ is irreducible in $\mathbb{Z}_7[x]$.

Question 16

You should be able to do this question after reading Chapter 18.

Determine which of the following elements of the field of order $7^2, \mathbb{F} = \mathbb{Z}_7(i)$ where $i^2 = -1$, is a primitive element of $\mathbb{F}$:

- $3 \cdot i + 3$
- i
- $2 \cdot i + 2$
- $-i - 3$

Enter the element from this list that is primitive in the box below.

Question 17

You should be able to do this question after reading Chapter 19.

Determine whether each of the following is an algebraic or transcendental element over $\mathbb{Q}$.

The element $3\pi + \pi^2$ is ____ element over the field $\mathbb{Q}(\pi)$.

The element $\sqrt[3]{e^7}$ is ____ element over the field $\mathbb{Q}$.

The element $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is ____ element over the field $\mathbb{Q}$.

Question 18

This question is based on material in Chapters 18 and 19.

Find the minimal polynomial of $x = 2 \cdot \sqrt{17} - 1$ over $\mathbb{Q}$.

The minimal polynomial is given by $p(x) =$ ____.

Question 19

This question is based on material in Chapters 18 and 19.

Find the minimum polynomial of $x = \sqrt{2} + \sqrt{7}$ over $\mathbb{Q}$.

The minimal polynomial is given by $p(x) =$ [ ].

Question 20

This question is based on material in Chapter 20.

Determine the missing numbers.

Suppose that (31,7,11) is an RSA triple so that the public key is (217,11). Alice wishes to send the message $m = 22$. Alice computes $c =$ [ ]. Bob uses his private key $d =$ [ ] to decrypt the message.

Question 21

This question is based on material in Chapter 20.

Determine the order of the group $(E, +)$ for the elliptic curve corresponding to the equation $y^2 = x^3 - x + 1$ over GF_7.

Answer: [ ]

Solutions

Solution to Question 1

True

In general, the ring $\mathbb{Z}_n$ is an integral domain if, and only if, n is a prime number.

An integral domain is a ring with no zero divisors (Definition 2.6 of Chapter 12, HB page 53). The ring $\mathbb{Z}_n$ consists of the set of integers $\{0, 1, \ldots, n-1\}$ with addition and multiplication taken modulo n. This ring will have zero divisors if, and only if, we can find two integers, $a, b \in \{0, 1, \ldots, n-1\}$ with $a \times b = 0 \pmod{n}$.

If n is not prime then $n = a \times b$ for some $a, b < n$. Hence $a \times b = 0 \in \mathbb{Z}_n$ and $\mathbb{Z}_n$ is not an integral domain.

Now assume that n is prime. If $a \times b = 0 \in \mathbb{Z}_n$ then n must divide the product ab and, by Euclid's Lemma for prime factors (Theorem 1.4 of Chapter 2, HB page 17), n must divide either a or b which is a contradiction since a and b are both strictly less than n.

Therefore the ring $\mathbb{Z}_n$ is an integral domain if, and only if, n is prime. Hence it is true that $\mathbb{Z}_{11}$ is an integral domain.

In fact $\mathbb{Z}_n$ is a field (Definition 1.14 of Chapter 11, HB page 47) if, and only if n is prime (Corollary 1.19 of Chapter 11). Since all fields are integral domains (Lemma 1.17 of Chapter 11) this shows that $\mathbb{Z}_n$ is an integral domain if n is prime. However this does not show that $\mathbb{Z}_n$ is an integral domain *only if* n is prime since not all integral domains are fields. All non-zero elements must have a multiplicative inverse in a field and this is not necessarily true in an arbitrary integral domain. The ring of integers, $\mathbb{Z}$, and the ring of polynomials over $\mathbb{Z}$, $\mathbb{Z}[x]$ are both examples of integral domains that are not fields (Example 2.9(a), Theorem 4.11 and Definition 4.1 of Chapter 12, HB page 55).

Solution to Question 2

The correct answers are as follows.

Let R be a commutative ring. We say that a non-zero element $x \in R$ is **prime** (Definition 2.6 of Chapter 12, HB page 53) if whenever x divides a product, $yz \in R$, with $y, z \in R$ then x divides one of y or z.

Let R be a commutative ring. We say that a non-zero element $x \in R$ is **irreducible** (Definition 2.5 of Chapter 12, HB page 53) if it is not a unit and if we cannot write x as a product, $x = yz$, with $y, z \in R$ unless one of y or z is a unit.

Let R be a commutative ring. If a non-zero element $x \in R$ has a multiplicative inverse then we say that x is a **unit** (Definition 1.13 of Chapter 11, HB page 47).

Let R be a commutative ring. If $x = u \times y$ where u is a unit then we say that x is an **associate** of y (Definition 2.3 of Chapter 12, HB page 52).

Solution to Question 3

In a Euclidean domain it is always true that if $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$. This is always true because all Euclidean domains are integral domains (Definition 3.1 of Chapter 12, HB page 54). If R is an integral domain then R has no zero divisors (Definition 2.8 of Chapter 12, HB page 53) and this means that if $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$.

A Euclidean domain is also a ring (Definition 1.1 of Chapter 11, HB page 46) and so it is always true that R is closed under addition and multiplication, addition is commutative and R has an additive identity. (In other words for all a and b in R, we have $a + b, a \times b \in R; a + b = b + a$ and there is an element $0 \in R$ with $a + 0 = a$.)

It is always true that there exists a function $N : R\{0\} \to \mathbb{N} \cup \{0\}$ such that for non-zero $a, b \in R$ we have $N(a) \leq N(ab)$ and there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$. A Euclidean domain is an integral domain in which this is always

true (Definition 3.1 of Chapter 12, HB page 54). All Euclidean domains are integral domains but not all integral domains are Euclidean domains. $\mathbb{Z}[\sqrt{-5}]$ is an example of an integral domain upon which we cannot define a Euclidean norm (and so $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a Euclidean domain (Worked Exercise 3.9 of Chapter 12, page 200 of Book C)).

It is always true that every non-zero non-unit element of R can be written as a product of irreducibles and this product is unique up to associates. An integral domain in which this is true is a unique factorisation domain (Definition 4.1 of Chapter 12, HB page 55) and all Euclidean domains are unique factorisation domains (Theorem 4.5 of Chapter 12, HB page 55). Note that not all unique factorisation domains are Euclidean domains. $\mathbb{Z}[x]$ is an example of a unique factorisation domain that is not a Euclidean domain (Exercise 3.3 and Theorem 4.11 of Chapter 12 (Book C page 201 and HB page 55)).

It is not always true that the multiplicative identity, 1, of R, is not equal to the additive identity 0, and all elements of R have a multiplicative inverse. In other words for all $r \in R$ we can find an element $s \in R$ with $r \times s = s \times r = 1$. A ring (with a 1) where this also holds is a field (Definition 1.14 of Chapter 11, HB page 47). All fields are Euclidean domains but not all Euclidean domains are fields. $\mathbb{Q}[x]$, the ring of polynomials in x with rational coefficients is an example of a Euclidean domain that is not a field (Lemma 2.9 of Chapter 11 (HB page 48) and Example 3.2(c) of Chapter 12 (Book C page 195)).

Solution to Question 4

See the diagram on page 33 of Chapter 17 (HB page 96).

Solution to Question 5

$A = \{2m_1 + 2m_2 i : m_1, m_2 \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}[i]$. To see this, first note that A is clearly non-empty and then note that $A = 2\mathbb{Z}[i]$ (see Definition 2.5 of Chapter 17, HB page 94, and the discussion about this definition in Book E).

$A = \{0, 4\}$ is an ideal of $\{0, 1, 2, 3, 4, 5, 6, 7\}$. By inspection it is clearly non-empty and equal to $4R = \{4r : r \in R\}$ (see Definition 2.5 of Chapter 17, HB page 94, and the discussion about this definition in Book E).

$A = \{\text{polynomials } p(x) \text{ in } \mathbb{Q}[x] \text{ with } p(4) = 0\}$ is an ideal of $\mathbb{Q}[x]$. First it is clearly non-empty. Also by the Factor Theorem that is Theorem 4.2 of Chapter 11 (HB page 50) $A = (x - 4)\mathbb{Q}[x]$ (see Exercise 2.3 of Chapter 17).

$A = \{2^n \in \mathbb{Z} : n \in \mathbb{N}\}$ is not an example of an ideal of $\mathbb{Z}$ since, for example, we have $2 \in A$ and $8 \in A$ but $8 - 2 = 6 \notin A$ so A does not satisfy the conditions listed in Definition 2.1 of Chapter 17 (HB page 94).

$A = \{\pm p : p \text{ is prime}\} \cup \{0\}$ is not an ideal of $\mathbb{Z}$ since, for example, 5 and $11 \in A$ but $11 - 5 = 6 \notin A$ so A does not satisfy the conditions listed in Definition 2.1 of Chapter 17 (HB page 94).

Solution to Question 6

The answer is 2.

Since $\mathbb{Z}$ is a principal ideal domain, we know from Lemma 3.7 of Chapter 17 (HB page 97) that a must be the highest common factor of 2 and 10.

Solution to Question 7

The kernel of $f : M_2 \to \mathbb{Z}$ is the ideal of M_2 consisting of all matrices in M_2 that map to $0 \in \mathbb{Z}$. In this case this is $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & z \end{pmatrix} : z \in \mathbb{Z} \right\} \subseteq M_2$. Since this is not the zero ideal we see that f is not one-one (Definition 4.11, Proposition 4.12 and Proposition 4.14 of Chapter 17, HB page 99). $\mathrm{Ker}(f)$ is an ideal of M_2 (Proposition 4.14 of Chapter 17, HB page 99) and an ideal of a ring is an additive subgroup (HB page 94, Properties of ideals). (Aside: in fact a ring homomorphism $f : R \to S$ can be considered as a group homomorphism from the additive group of R to the additive group of S (compare Definition 4.9 of Chapter 5, HB page 29 with Definition 4.11 of Chapter 17, HB page 99)).

The image of $f : M_2 \to \mathbb{Z}$ is the subring of $\mathbb{Z}$ consisting of all elements of $\mathbb{Z}$ that are equal to $f\begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix}$ for M_2 for some $z_i \in \mathbb{Z}$. In this case this is all of $\mathbb{Z}$ (showing that f is onto) (Definition 4.11, Proposition 4.12 and Proposition 4.14 of Chapter 17, HB page 99).

Solution to Question 8

See the diagram on page 33 of Chapter 17 (HB page 96). See also Chapter 12, Definition 4.1 (HB page 55).

The correct answers are: a field, a Euclidean domain, a unique factorisation domain, and a principal ideal domain.

Solution to Question 9

The correct answers are $-i$, i and 1.

$N(5-8i) = 89 > 58 = N(7+3i)$, so we divide $5-8i$ by $7+3i$.

Rationalising the denominator gives

$$\frac{5-8i}{7+3i} = \frac{5-8i}{7+3i} \times \frac{7-3i}{7-3i} = \frac{11}{58} - \frac{71}{58}i,$$

so we guess at
$5-8i = (0-i)(7+3i) + a + bi$.

Solving this gives
$5-8i = (0-i)(7+3i) + (2-i)$.

Checking norms shows that this is okay, since $N(2-i) = 5 < 58 = N(7+3i)$.

We now divide $7+3i$ by $2-i$.

Rationalising the denominator gives

$$\frac{7+3i}{2-i} = \frac{7+3i}{2-i} \times \frac{2+i}{2+i} = \frac{11}{5} + \frac{13}{5}i,$$

so we guess at
$7+3i = (2+3i)(2-i) + c + di$.

Solving this gives $7+3i = (2+3i)(2-i) - i$.

Checking norms shows that this is okay, since $N(2-i) = 5 > 1 = N(-i)$.

Finally, $(2-1) = (1+2i)(-i) + 0$. So a hcf is $-i$. The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$ and hcfs are unique only up to multiplication by units (see text below Definition 3.6 of Chapter 12).

See Worked Exercises 2.14 of Chapter 17.

Solution to Question 10

In an integral domain all primes are irreducible but irreducibles are not always prime. $2 \in \mathbb{Z}[\sqrt{-5}]$ is not prime but is irreducible (see Exercise 2.5 of Chapter 12, page 193).

In a unique factorisation domain all primes are irreducible and all irreducibles are prime (Theorem 2.12 and Corollary 4.3 of Chapter 12, HB pages 53 and 55).

In a ring maximal ideals are prime. In a PID non-trivial prime ideals are maximal. (Lemma 1.17 of Chapter 11, Theorems 4.23 and 4.26 and Proposition 4.27 of Chapter 17 (HB pages 47, 99, 100))

Solution to Question 11

The answer is 12.

A primitive element of a finite field is a generator of the multiplicative group. By Corollary 3.5 of Chapter 18, HB page 106, the number of primitive elements in a field of order p^n is $\phi(p^n - 1)$, where ϕ is Euler's ϕ-function (Definition 3.1 of Chapter 9, HB page 42).

For the field of order 27, $p = 3$ and $n = 3$, so $p^n - 1 = 26 = 2 \times 13$.

Hence
$\phi(p^n - 1) = \phi(2) \times \phi(13) = 1 \times 12 = 12$.

See Corollary 3.5 of Chapter 18 (HB page 106) and Proposition 4.2 of Chapter 9 (HB page 43).

Solution to Question 12

This solution contains more detail than you would need to write. It follows the method used in Exercise 2.10 of Chapter 18 (page 104). The solution to this exercise indicates the level of detail expected in a solution to a question like this.

To show that $x^2 - 3$ is irreducible over $\mathbb{Q}[\sqrt{5}]$ we need to show that $x^2 - 3$ has no factors in $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$.

Since $x^2 - 3$ has degree 2 we know that any factor would be a linear factor of the form $(x - c)$ where $c \in \mathbb{Q}(\sqrt{5})$ is a root. Therefore to show that $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{5})$ it is sufficient to show that we cannot find an a and $b \in \mathbb{Q}$ with $(a + b\sqrt{5})^2 = 3$.

Assume (for a contradiction) that we can find an a and $b \in \mathbb{Q}$ with $(a + b\sqrt{5})^2 = 3$.

Then we have:

$$a^2 + 2ab\sqrt{5} + 5b^2 = 3.$$

Since $\sqrt{5} \notin \mathbb{Q}$ we must have either $a = 0$ or $b = 0$.

Case One: $a = 0$

If $a = 0$ then

$5b^2 = 3$ and so

$5^2b^2 = (5b)^2 = 15$ which is not possible for $b \in \mathbb{Q}$.

Therefore case one cannot occur and we must have $b = 0$.

Case Two: $b = 0$

If $b = 0$ then $a^2 = 3$ which is impossible for any $a \in \mathbb{Q}$.

Therefore $x^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{5})$.

Since $\sqrt{5} \notin \mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ and since $x^2 - 3$ is of degree 2 and is irreducible over $\mathbb{Q}(\sqrt{5})$ we have $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] = 2$.

Therefore, by the KLM Theorem (HB page 105)

$$[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] \times [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \times 2 = 4.$$

Solution to Question 13

There are various methods that may be used to find the multiplicative inverse of an element (see Worked Exercises 3.10 and 3.11 of Chapter 18).

This solution uses the method demonstrated in Worked Exercise 3.10(b) in which we multiply the given element by an arbitrary element of our field, assume that the result is equal to 1 and compare coefficients.

In this case the field is $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$. The polynomial $x^2 - x + 1$ is irreducible over $\mathbb{Z}_5$ and has degree 2.

Therefore Proposition 1.7 of Chapter 18 (HB page 101) tells us that an arbitrary element of $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$ can be written as $ax + b$. Therefore we want to find an element, $ax + b$ such that $(3x + 2)(ax + b) = 1$ in $\mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$.

In other words, when we reduce all coefficients modulo 5, and take into account the fact that $x^2 - x + 1 = 0$, then

$$(3x + 2)(ax + b) = 1.$$

We proceed as follows:

Assume that

$$(3x+2)(ax+b)=1.$$

Then

$$3ax^2+(2a+3b)x+2b=1.$$

Using the identity $x^2=x-1$ and substituting for x^2 gives

$$(3x+2)(ax+b)=(3a+3b+2a)x+(2b-3a)=1.$$

Comparing coefficients gives

$$5a+3b=0 \text{ and } 2b-3a=1.$$

Now $2b-3a=1$ tells us that $b=\frac{1+3a}{2}$ and substituting this into $5a+3b=0$ gives:

$$5a+3(\tfrac{1+3a}{2})=0$$

and so $10a+3+9a=0$. Hence (working modulo 5) we have $-a=-3$ and so $a=3$ and $b=0$.

Hence the multiplicative inverse of $3x+2$ in $\mathbb{Z}_5[x]/\langle x^2-x+1\rangle$ is $3x$.

(Notes

1. We can check this by multiplying: $3x(3x+2)=9x^2+6x$ and substituting $x^2=x-1$ gives $3x(3x+2)=9(x-1)+6x=1 \pmod 5$.
2. You do not have to show that x^2-x+1 is irreducible over $\mathbb{Z}_5[x]$ but this can be shown by calculating the value of x^2-x+1 when $x=\pm1, \pm2$ and 0 and noting that none of these is a root.)

Solution to Question 14

By Definition 2.1 of Chapter 17 (HB page 94), a non-empty set $I\subseteq R$ is an ideal of R if for all a,b in I and $r\in R$ we have $a-b\in I$ and $ra\in I$.

Hence $\{f(x)\in R : f(2)=f(5)=0\}$ and $\{f(x)\in R : f(2)=f'(2)=0\}$ are ideals in R.

Solution to Question 15

Since $\mathbb{Z}_7$ is a field, (Corollary 1.19 in Chapter 11, HB page 48) the polynomial ring $\mathbb{Z}_7[x]$ is a Euclidean domain (Example 3.2 in Chapter 12, also HB page 95, summary) and every Euclidean domain is a UFD (Corollary 2.11 and Theorem 2.16 in Chapter 17, HB page 95).

x^2+1 is irreducible in $\mathbb{Z}_7[x]$ since 6 is not a quadratic residue for 7 (and so x^2+1 has no roots in $\mathbb{Z}_7$ and, being of degree 2, cannot be factorised).

Figure 2.1 in Chapter 17 (HB page 96) should help determine some of the correct responses and the summary on page 95 of the HB is also useful.

Solution to Question 16

The definition of a primitive element is given in Definition 3.4 of Chapter 18 (HB page 106): α is a primitive element of the finite field $\mathbb{Z}_7(i)$ if it is a generator of the multiplicative group of the field.

The multiplicative order of any non-zero element of $\mathbb{Z}_7(i)$ must divide $7^2-1=48$ (Proposition 4.5, Chapter 5, HB page 29) and so the only possible multiplicative orders of an element that is not the multiplicative identity are $2,3,4,6,8,12,16,24$ and 48. In the calculations below we must remember that we are working in the finite field $\mathbb{Z}_7(i)$. The elements of this field are of the form $a+bi$ where a and b are elements of $\mathbb{Z}_7$ and so a and b are calculated (mod 7). Therefore when we say (mod 7) we mean that we are writing the element as $a+bi$ and calculating a and b mod 7.

So calculating $(2 \cdot i + 2)^n \pmod 7$ for $n = 2, 3, 4, 6, 8, 12, 16, 24$, we obtain

$$\begin{aligned}(2 \cdot i + 2)^2 &\equiv i \pmod 7,\\ (2 \cdot i + 2)^4 &\equiv 6 \pmod 7,\\ (2 \cdot i + 2)^8 &\equiv 1 \pmod 7,\\ (2 \cdot i + 2)^{16} &\equiv 1 \pmod 7,\\ (2 \cdot i + 2)^3 &\equiv 2 \cdot i + 5 \pmod 7,\\ (2 \cdot i + 2)^6 &\equiv 6 \cdot i \pmod 7,\\ (2 \cdot i + 2)^{12} &\equiv 6 \pmod 7,\\ (2 \cdot i + 2)^{24} &\equiv 1 \pmod 7,\end{aligned}$$

and so $(2 \cdot i + 2)^8 \equiv 1 \pmod 7$ meaning that $2 \cdot i + 2$ is not a primitive element.

We also notice that $i = (2 \cdot i + 2)^2 \pmod 7$ and so i is not a primitive element.

Similarly calculating $(3 \cdot i + 3)^n \pmod 7$ for $n = 2, 3, 4, 6, 8, 12, 16, 24$, we obtain

$$\begin{aligned}(3 \cdot i + 3)^2 &\equiv 4 \cdot i \pmod 7,\\ (3 \cdot i + 3)^4 &\equiv 5 \pmod 7,\\ (3 \cdot i + 3)^8 &\equiv 4 \pmod 7,\\ (3 \cdot i + 3)^{16} &\equiv 2 \pmod 7,\\ (3 \cdot i + 3)^3 &\equiv 5 \cdot i + 2 \pmod 7,\\ (3 \cdot i + 3)^6 &\equiv 6 \cdot i \pmod 7,\\ (3 \cdot i + 3)^{12} &\equiv 6 \pmod 7,\\ (3 \cdot i + 3)^{24} &\equiv 1 \pmod 7,\end{aligned}$$

and so $(3 \cdot i + 3)^{24} \equiv 1 \pmod 7$ meaning that $(3 \cdot i + 3)$ is not a primitive element.

Finally calculating $(-i - 3)^n \pmod 7$ for $n = 2, 3, 4, 6, 8, 12, 17, 24$, we obtain

$$\begin{aligned}(-i - 3)^2 &\equiv 6 \cdot i + 1 \pmod 7,\\ (-i - 3)^4 &\equiv 5 \cdot i \pmod 7,\\ (-i - 3)^8 &\equiv 3 \pmod 7,\\ (-i - 3)^{16} &\equiv 2 \pmod 7,\\ (-i - 3)^3 &\equiv 2 \cdot i + 3 \pmod 7,\\ (-i - 3)^6 &\equiv 5 \cdot i + 5 \pmod 7,\\ (-i - 3)^{12} &\equiv i \pmod 7,\\ (-i - 3)^{24} &\equiv 6 \pmod 7,\end{aligned}$$

and none of these are congruent to 1 (mod 7). Hence $-i - 3$ is a generator of the multiplicative group of $\mathbb{F} = \mathbb{Z}_7(i)$ and is therefore a primitive element. (See Exercise 3.3 of Chapter 18, Book E page 110. Note that although we have listed all of the calculations above, showing that $a^r = 1$ for any $r < 48$ proves that α is not a primitive element.)

[In fact, Corollary 3.3 of Chapter 18 tells us that there are $\phi(7^2 - 1) = 16$ primitive elements in $\mathbb{Z}_7(i)$.]

Solution to Question 17

By Definition 2.11 of Chapter 18 (HB page 104), α is an algebraic element of a field F if there is a polynomial $f(x)$ in $F[x]$ such that $f(\alpha) = 0$. If there is no such polynomial, then the element is transcendental.

$3\pi + \pi^2$ is a root of the polynomial $f(x) = x - 3\pi - \pi^2$, which is in $\mathbb{Q}(\pi)[x]$.

By Theorem 1.11 of Chapter 19 (HB page 110), since e is transcendental and 3 and 7 are coprime, then $\sqrt[3]{e^7}$ is transcendental.

$-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a root of the polynomial $g(x) = x^2 + x + 1$, which is in $\mathbb{Q}[x]$.

Solution to Question 18

The definition of a minimal polynomial is Definition 2.22 of Chapter 18 (HB page 105).

Our goal is to find a monic polynomial with coefficients in $\mathbb{Q}$ for which $2 \cdot \sqrt{17} - 1$ is a root.

Since $2 \cdot \sqrt{17} - 1 \notin \mathbb{Q}$, any polynomial over $\mathbb{Q}$ for which it is a root must have degree at least two. Hence if we find a monic polynomial of degree two that has $x = 2 \cdot \sqrt{17} - 1$ as a root, then this polynomial must be the minimal polynomial for $x = 2 \cdot \sqrt{17} - 1$.

The key is to note that $(x + 1)^2 - (2 \cdot \sqrt{17})^2$ is a polynomial of degree two over $\mathbb{Q}$ that has

$2 \cdot \sqrt{17} - 1$ as a root and so, on expanding and simplifying, we conclude that

$$x^2 + 2 \cdot x - 67$$

is the minimal polynomial for $2 \cdot \sqrt{17} - 1$.

Solution to Question 19

Worked Exercise 1.6 of Chapter 19 shows a fully worked example.

Following the method of this worked exercise, we let $x = \sqrt{2} = \sqrt{7}$.

Since $\sqrt{2}$ satisfies the irreducible quadratic equation $x^2 - 2 = 0$ over $\mathbb{Q}$, we conclude that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Now $\sqrt{7} \notin \mathbb{Q}(\sqrt{2})$ (since if $\sqrt{7} = a + b\sqrt{2}$, then squaring both sides and rearranging gives $\sqrt{2} \in \mathbb{Q}$, a contradiction) and $\sqrt{7}$ is a root of $x^2 - 7 = 0$, an irreducible equation over $\mathbb{Q}(\sqrt{2})$, and so $[\mathbb{Q}(\sqrt{7}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$.

Hence by the KLM theorem (Theorem 2.29 of Chapter 18, HB page 105), we deduce that $[\mathbb{Q}(\sqrt{7}, \sqrt{2}), \mathbb{Q}] = 4$ and so we are looking for 4 basis elements. The proof of the KLM theorem tells us that we can obtain these basis elements by taking products of the basis elements for $\mathbb{Q}(\sqrt{7}, \sqrt{2})$ considered as a vector space over $\mathbb{Q}(\sqrt{2})$ with the basis elements for $\mathbb{Q}(\sqrt{2})$ considered as a vector space over $\mathbb{Q}$.

A basis for $\mathbb{Q}(\sqrt{7}, \sqrt{2})$ considered as a vector space over $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{7}\}$ and a basis for $\mathbb{Q}(\sqrt{2})$ considered as a vector space over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$.

Hence, taking products gives us $\{1, \sqrt{2}, \sqrt{7}, \sqrt{2} \cdot \sqrt{7}\}$ as a basis for $\mathbb{Q}(\sqrt{7}, \sqrt{2})$ as a vector space over $\mathbb{Q}$. Thus we know our minimal polynomial has degree at most 4.

We know that all elements of $\mathbb{Q}(\sqrt{7}, \sqrt{2})$ can be written as a linear combination of our basis elements. In particular, we can take the product of each of our basis elements with x to find:

$$\begin{aligned}
x &= 0 \times 1 + 1 \times \sqrt{2} + 1 \times \sqrt{7} + 0 \times \sqrt{2} \cdot \sqrt{7} \\
x\sqrt{2} &= 2 \times 1 + 0 \times \sqrt{2} + 0 \times \sqrt{7} + 1 \times \sqrt{2} \cdot \sqrt{7} \\
x\sqrt{7} &= 7 \times 1 + 0 \times \sqrt{2} + 0 \times \sqrt{7} + 1 \times \sqrt{2} \cdot \sqrt{7} \\
x\sqrt{2} \cdot \sqrt{7} &= 0 \times 1 + 7 \times \sqrt{2} + 2 \times \sqrt{7} + 0 \times \sqrt{2} \cdot \sqrt{7}
\end{aligned}$$

and so

$$\begin{aligned}
x - x &= 0 \times 1 + 1 \times \sqrt{2} + 1 \\
&\quad \times \sqrt{7} + 0 \times \sqrt{2} \cdot \sqrt{7} - x \\
x\sqrt{2} - x\sqrt{2} &= 2 \times 1 + 0 \times \sqrt{2} + 0 \\
&\quad \times \sqrt{7} + 1 \times \sqrt{2} \cdot \sqrt{7} - x\sqrt{2} \\
x\sqrt{7} - x\sqrt{7} &= 7 \times 1 + 0 \times \sqrt{2} + 0 \\
&\quad \times \sqrt{7} + 1 \times \sqrt{2} \cdot \sqrt{7} - x\sqrt{7} \\
x\sqrt{2} \cdot \sqrt{7} - x\sqrt{2} \cdot \sqrt{7} &= 0 \times 1 + 7 \times \sqrt{2} + 2 \times \sqrt{7} + 0 \\
&\quad \times \sqrt{2} \cdot \sqrt{7} - x\sqrt{2} \cdot \sqrt{7}
\end{aligned}$$

In other words, we have the system of equations $\mathbf{Ab} = \mathbf{0}$, where $\mathbf{b}$ is the vector consisting of the basis elements and

$$\mathbf{A} = \begin{pmatrix} -x & 1 & 1 & 0 \\ 2 & -x & 0 & 1 \\ 7 & 0 & -x & 1 \\ 0 & 7 & 2 & -x \end{pmatrix}$$

We know that x exists and is non-zero (since $x = \sqrt{2} + \sqrt{7}$) and so the determinant of the matrix $\mathbf{A}$ must be zero, $\det(\mathbf{A}) = 0$.

Using elementary row and column operations, we find that

$$\det(\mathbf{A}) = x^4 - 18 \cdot x^2 + 25$$

and so the polynomial $x^4 - 18 \cdot x^2 + 25$ (which is of degree 4) must be the minimal polynomial over $\mathbb{Q}$ that has root $\sqrt{2} + \sqrt{7}$.

Solution to Question 20

Using the notation of the text following Definition 1.11 on page 200 of Book E (HB page 113) we have $p = 31$, $q = 7$, $n = pq = 217, \phi(n) = 180$ and e was chosen to be 11.

Hence (following the RSA encryption/decryption instructions given on page 113 of the HB), the ciphertext c is given by $c \equiv 22^{11} \pmod{217} = 141$ and the private key d is 131 (since $11 \times 131 \equiv 1 \bmod(180)$).

Solution to Question 21

Elliptic curves are defined in Chapter 20, Definition 2.3 (HB page 115). Worked Exercise 2.17 on page 230 of Book E may be helpful.

We are working over $GF_7(= \mathbb{Z}_7) = \{0, \pm 1, \pm 2, \pm 3\}$.

Substituting each of these elements into the equation $f(x) = x^3 - x + 1$ (working mod 7) gives the following:

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 1, f(-1) = 1, \\ f(2) &= 0, f(-2) = 2, \\ f(3) &= -3, f(-3) = -2. \end{aligned}$$

Since we need $f(x) = y^2$, we look for the values of x which give us quadratic residues of 7. The quadratic residues of 7 are 0, 1, 2 and -3 so $x = 0, \pm 1, 2, -2$ and 3 will work. Taking square roots (mod 7) gives us the corresponding y-values. Therefore we get the group elements $\{\mathcal{O}, (0, \pm 1), (-1, \pm 1), (1, \pm 1), (2, 0), (-2, \pm 3), (3, \pm 2)\}$ and the order of the group is 12.

The Open University

M303

Further pure mathematics

Practice Quiz 6

Question 1

This question revises material that is in Book D.

Let $X = (0,1) \cup (2,3]$ and let d be the metric on X induced by the usual Euclidean metric for $\mathbb{R}$.

Determine which of the expressions 'open but not closed', 'closed but not open', 'not closed and not open', 'closed and open' should go in the blank spaces. You may use expressions more than once.

1. The subset $[\frac{5}{2}, 3)$ is [ ] when considered as a subset of (X, d).
2. The subset $(\frac{5}{2}, 3)$ is [ ] when considered as a subset of (X, d).
3. The subset $(0, 1)$ is [ ] when considered as a subset of (X, d).
4. The subset $\{\frac{1}{n+1} : n \in \mathbb{N}\}$ is [ ] when considered as a subset of (X, d).
5. The subset $(2, 3]$ is [ ] when considered as a subset of (X, d).

Question 2

In each of the following you are given a metric space (X, d) and sets $E \subseteq A \subseteq X$.

Select those of the following for which E is a d_A-closed subset of A, where d_A is the metric induced on A by d.

$(X, d) = (\mathbb{R}, d_0)$, where d_0 is the discrete metric, $A = (2, 3)$, and $E = \mathbb{Q} \cap (2, 3)$.

$(X, d) = (\mathbb{R}, d^{(1)})$, $A = (2, 3)$, and $E = \mathbb{Q} \cap (2, 3)$.

$(X, d) = (\mathbb{R}^2, d^{(2)})$, $A = \{(x, y) : x^2 + y^2 < 1\} \cup \{(x, y) : y > 3\}$, and $E = \{(x, y) : x^2 + y^2 < 1\}$.

$(X, d) = (C[0, 1], d_{\max})$, $A = \{f \in C[0, 1] : |f(x)| < 1$, for each $x \in [0, 1]\}$, and $E = \{f \in A : f(0) = 0\}$.

Question 3

For which of the following metric spaces (X, d) does the pair of subsets $\{A, B\}$ form a disconnection?

Select *all* that apply.

$X = [0, 1] \cup \{1 + \frac{1}{n} : n \in \mathbb{N}\}, d = d_X^{(1)}$, $A = [0, 1]$ and $B = \{1 + \frac{1}{n} : n \in \mathbb{N}\}$.

$X = \{\frac{1}{n} : n \in \mathbb{N}\}, d = d_X^{(1)}$, $A = \{\frac{1}{2n} : n \in \mathbb{N}\}$ and $B = \{\frac{1}{2n-1} : n \in \mathbb{N}\}$.

$X = \mathbb{R}$, d is the discrete metric on X, $A = \mathbb{Q}$ and $B = \mathbb{R} - \mathbb{Q}$.

$X = [0, 1) \cup (1, 2], d = d_X^{(1)}, A = [0, 1)$ and $B = (1, 2]$.

$X = \{1\} \cup (1, 2), d = d_X^{(1)}, A = \{1\}$ and $B = (1, 2)$.

Question 4

Is the following statement true or false?

It is not possible for a subspace of $(\mathbb{R}^n, d^{(n)})$ to be homeomorphic to a subspace of $(\mathbb{R}^m, d^{(m)})$ unless $n = m$.

Question 5

Fill each of the blanks with the correct phrase chosen from the following: 'an open cover', 'not a cover', 'a cover, which is open'.

$\{A_r : r \in \mathbb{R}\}$ where $A_r = \{(x, r) : x \in \mathbb{R}\}$ is [ ] of $\mathbb{R}^2$ in $(\mathbb{R}^2, d^{(2)})$.

$\{B_n : n \in \mathbb{N}\}$ where $B_n = \{(x, y) : x^2 + y^2 > \frac{1}{n}\}$ is [ ] of $\mathbb{R}^2$ in $(\mathbb{R}^2, d^{(2)})$.

$\{C_n : n \in \mathbb{N}\}$ where $C_n = \{(x, y) : x^2 + y^2 < 4 - \frac{1}{n}\}$ is [ ] of $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$ in $(\mathbb{R}^2, d^{(2)})$.

Question 6

This question asks you to check whether one of the 3 conditions of the Arzelà-Ascoli Theorem (that is Theorem 3.12 of Chapter 22, HB page 131) holds for a given set A.

Let
$A = \{f \in C[0, 1] : |f(x) - f(y)| \leq 4|x - y|^{\frac{1}{5}}\}$.

Determine whether A is an equicontinuous family of functions.

This question is designed to help you to practise writing a full solution to a question so you will get the maximum benefit from this question if you write out a full answer.

Question 7

This question asks you to check whether one of the 3 conditions of the Arzelà-Ascoli Theorem (that is Theorem 3.12 of Chapter 22, HB page 131) holds for a given set A.

Let $A = \{f \in C[0, 1] : f(\frac{1}{5}) = 4$ and $|f(x) - f(y)| \leq 3|x - y|^5\}$.

Determine whether A is $d_{\max}$-closed (Definition 5.1 of Chapter 15, HB page 79).

This question is designed to help you to practise writing a full solution to a question so you will get the maximum benefit from this question if you write out a full answer. (You may find it helpful to look at Worked Exercise 3.3 of Chapter 22, Book F, page 94.)

Question 8

Write appropriate expressions from the lists below to fill the blank spaces and correctly complete the statements.

It is [ ] that any closed and bounded metric space is compact.

[ ] is given by

[ ].

It is [ ] that an open and bounded metric space is never compact.

[ ] is given by

[ ].

It is [ ] that an unbounded metric space is never compact.

[ ] is given by

[ ].

Let $A = \mathbb{N}, B = \{\frac{1}{n} : n \in \mathbb{N}\}$ and $C = \{1, 2, 3, 4, 5\}$.

true, false An example, A counterexample

(B, d_0), where d_0 is the discrete metric
(C, d_0), where d_0 is the discrete metric
(A, d), where d denotes the metric induced on A by the Euclidean metric
(B, d), where d denotes the metric induced on B by the Euclidean metric

Question 9

Write the correct one of 'true' or 'false' in the blank space to make each statement true.

It is [ ] that $(1, \infty)$ with the induced Euclidean metric is a complete metric space.

It is [ ] that $\{f \in C[0,1] : |f(\frac{1}{2})| = 0 \text{ and } |f(x)| \leq 2\}$, with the $d_{\max}$ metric, is a complete metric space.

Question 10

Correctly complete the following table by writing either 'yes' or 'no' in each of the nine empty spaces.

Set	**Metric**, d	d -connected?	d -compact?	d -complete?
$(\mathbb{R} - \mathbb{Z})$	d_0			
$X = \{\frac{1}{n} : n \in \mathbb{Z} - \{0\}\} \cup \{0\}$	$d_X^{(1)}$			
$\mathbb{R}^2 - \mathbb{Q}^2$	$d^{(1)}_{\mathbb{R}^2 - \mathbb{Q}^2}$			

Question 11

Let $A = \{(x, y) \in \mathbb{R}^2 : |x| \leq 5 \text{ and } |y| \leq 1\}$ and

$B = \{(x, y) \in \mathbb{R}^2 : |x| \leq 2 \text{ and } |y| \leq 4\}$.

Find $d_H(A, B)$, where d_H is the Hausdorff metric for $\mathcal{K}(\mathbb{R}^2)$.

$d_H(A, B) =$ [ ]

Question 12

This question is worth 2 marks.

Define $S_1, S_2, S_3 : \mathbb{R} \to \mathbb{R}$ by

$$S_1(x) = \tfrac{1}{9}x, \; S_2(x) = \tfrac{1}{3}x + \tfrac{1}{3}, \; S_3(x) = \tfrac{1}{3}x + \tfrac{2}{3}.$$

Find the dimension of the non-empty compact invariant set K for the iterated function scheme $\{S_1, S_2, S_3\}$.

Give an *exact* answer, decimal approximations are not acceptable.

$\dim(K) =$ [ ].

Solutions

Solution to Question 1

By Theorem 2.1 of Chapter 21 (HB page 119) and the characterisation of closed sets given on page 120 of the Handbook, we have that $A \subseteq X$ is open/closed in $X \subseteq \mathbb{R}$ if we can find an open/closed set, $A' \subseteq \mathbb{R}$ with $A = A' \cap X$.

Intervals of the form $[a, b]$ are closed in $\mathbb{R}$, and intervals of the form (a, b) are open in $\mathbb{R}$, with respect to the usual Euclidean metric (table on HB page 89).

1. $[\frac{5}{2}, 3)$ is not open, since any open ball, $B_d(\frac{5}{2}, r)$, around the point $\frac{5}{2}$ contains the point $\frac{5}{2} - \frac{r'}{2}$, where $r' = \min\{r, \frac{1}{2}\}$, and this point is in X but not in $[\frac{5}{2}, 3)$.

   It is not closed, since the sequence $(3 - \frac{1}{n+1})_{n\in\mathbb{N}}$, converges to the point $3 \notin [\frac{5}{2}, 3)$ but which is in X.
2. $(\frac{5}{2}, 3) = (\frac{5}{2}, 3) \cap X$ is open.

   It is not closed, since the sequence $(\frac{5}{2} + \frac{1}{n+2})_{n\in\mathbb{N}}$, converges to the point $\frac{5}{2} \notin (\frac{5}{2}, 3)$ but which is in X.
3. $(0, 1)$ is open, since $(0, 1) = (0, 1) \cap X$ and $(0, 1)$ is closed, since $(0, 1) = [0, 1] \cap X$.
4. $\{\frac{1}{n+1} : n \in \mathbb{N}\}$ is closed. The closure of this set in $\mathbb{R}$ is $\{0\} \cup \{\frac{1}{n+1} : n \in \mathbb{N}\}$ and $(\{0\} \cup \{\frac{1}{n+1} : n \in \mathbb{N}\}) \cap X = \{\frac{1}{n+1} : n \in \mathbb{N}\}$.

   $\{\frac{1}{n+1} : n \in \mathbb{N}\}$ is not open, since, for example, the open ball in X, $B_d(\frac{1}{2}, r)$, contains the interval $[\frac{1}{2} - \delta, \frac{1}{2} + \delta]$, where $\delta = \min\{r, \frac{1}{4}\}$ which, by the density property of the reals (HB page 7), contains an irrational number that cannot be in $\{\frac{1}{n+1} : n \in \mathbb{N}\}$.
5. $(2, 3]$ is open, since $(2, 3] = (2, 4) \cap X$ and $(2, 3]$ is closed since $(2, 3] = [2, 3] \cap X$.

The correct answer is:

1. The subset $[\frac{5}{2}, 3)$ is [not closed and not open] when considered as a subset of (X, d).
2. The subset $(\frac{5}{2}, 3)$ is [open but not closed] when considered as a subset of (X, d).
3. The subset $(0, 1)$ is [closed and open] when considered as a subset of (X, d).
4. The subset $\{\frac{1}{n+1} : n \in \mathbb{N}\}$ is [closed but not open] when considered as a subset of (X, d).
5. The subset $(2, 3]$ is [closed and open] when considered as a subset of (X, d).

Solution to Question 2

Characterisations of closed sets are given on page 120 of the HB.

There were 3 correct options.

$(X, d) = (\mathbb{R}, d^{(2)})$;
$A = \{(x, y) : x^2 + y^2 < 1\} \cup \{(x, y) : y > 3\}; d_A$ is the metric on A induced by the Euclidean metric on $\mathbb{R}^2$.

Then $E = \{(x, y) : x^2 + y^2 < 1\}$ is a d_A-closed subset of A.

The d_A-closed sets of A are the intersections of the $d^{(2)}$-closed subsets of $\mathbb{R}^2$ with A.

The set $E' = \{(x, y) : x^2 + y^2 \leq 1\}$ is a $d^{(2)}$-closed subset of $\mathbb{R}^2$ since it is $B_{d^{(2)}}[(0, 0), 1]$, the closed ball around $\mathbf{0}$ (Proposition 1.3 Chapter 16, HB page 80).

Therefore since $E = E' \cap A$ we have that E is d_A-closed.

$(X, d) = (\mathbb{R}, d_0); A = (2, 3); d_A$ is the metric on A induced by the discrete metric on $\mathbb{R}$.

Then $E = \mathbb{Q} \cap (2, 3)$ is a d_A-closed subset of A since the metric on A induced by the discrete metric on $\mathbb{R}$ makes A into a discrete metric space and all sets in any discrete metric space are both open and closed.

$(X, d) = (\mathbb{R}, d^{(1)}); A = (2, 3); d_A$ is the metric induced by the Euclidean metric on $\mathbb{R}$.

Let $E = \mathbb{Q} \cap (2, 3)$. Consider the point $\sqrt{5} \in A - E$. The sequence (a_n), of rational

points in $(2,3)$, given by $a_n = \sqrt{5}$ rounded to n decimal places, has $\sqrt{5}$ as a limit and so (a_n) is a sequence of terms in E that is d_A-convergent to a point not in E. Therefore E is not d_A-closed.

$(X,d) = (C[0,1], d_{\max})$,
$A = \{f \in C[0,1] : |f(x)| < 1 \text{ for all } x\}$; d_A is the metric induced by the max metric on $C[0,1]$.

Let $E = \{f \in A : f(0) = 0\}$. Then $E = E' \cap A$ where $E' = \{f \in C[0,1] : f(0) = 0\}$.

E' is a $d_{\max}$-closed subset of $C[0,1]$ from Chapter 16 (Exercise 1.9).

Therefore E is d_A-closed.

The correct answer is: $(X,d) = (\mathbb{R}^2, d^{(2)})$,
$A = \{(x,y) : x^2 + y^2 < 1\} \cup \{(x,y) : y > 3\}$,
and $E = \{(x,y) : x^2 + y^2 < 1\}$.
$(X,d) = (\mathbb{R}, d_0)$, where d_0 is the discrete metric, $A = (2,3)$, and $E = \mathbb{Q} \cap (2,3)$.
$(X,d) = (C[0,1], d_{\max})$,
$A = \{f \in C[0,1]| : |f(x)| < 1$, for each $x \in [0,1]\}$, and $E = \{f \in A : f(0) = 0\}$.

Solution to Question 3

For the definitions and characterisations of connectedness see Definition 3.1, Definition 3.11 and Proposition 3.4 of Chapter 21 (HB pages 120 and 121).

For the characterisations of open and closed sets see Handbook page 120, and Theorem 2.1 of Chapter 21 (HB page 119).

$(X,d) = (\{1\} \cup (1,2), d) = ([1,2), d_X^{(1)})$,
$A = \{1\}$ and $B = (1,2)$.

For $\{\{1\},(1,2)\}$ to be a disconnection, we would need $\{1\}$ and $(1,2)$ to each be simultaneously d-open and d-closed. The sequence given by $a_n = 1 + \frac{1}{n+1}$ has terms in $(1,2)$ and is $d^{(1)}$-convergent to $1 \notin (1,2)$. Therefore $(1,2)$ is not d-closed and $\{A,B\}$ is not a disconnection.

$X = \{\frac{1}{n} : n \in \mathbb{N}\}, d = d_X^{(1)}, A = \{\frac{1}{2n} : n \in \mathbb{N}\}$ and $B = \{\frac{1}{2n-1} : n \in \mathbb{N}\}$.

Certainly $A \cap B = \phi$ and $A \cup B = X$. For $\{A,B\}$ to be a disconnection for X, it is enough that A and B are both $d_X^{(1)}$-open.

Now $A = \left(\bigcup_{n=1}^{\infty} (\frac{1}{2n+1}, \frac{1}{2n-1})\right) \cap X$ and $\bigcup_{n=1}^{\infty} (\frac{1}{2n+1}, \frac{1}{2n-1})$ being the union of open intervals, is $d^{(1)}$-open. Hence A is d-open.

Similarly, $B = \left((\frac{1}{2}, 2) \cup \bigcup_{n=2}^{\infty} (\frac{1}{2n}, \frac{1}{2n-2})\right) \cap X$ and $(\frac{1}{2}, 2) \cup \bigcup_{n=2}^{\infty} (\frac{1}{2n}, \frac{1}{2n-2})$, being the union of open intervals, is $d^{(1)}$-open. Hence B is d-open.

We conclude that $\{A,B\}$ is a disconnection of X.

$(X,d) = ([0,1) \cup (1,2], d_X^{(1)})$, $A = [0,1)$ and $B = (1,2]$.

$\{A,B\}$ is a disconnection: clearly $A \cap B = \phi$ and $A \cup B = X$. Moreover,
$[0,1) = (-1,1) \cap X$ so is d-open in X and $(1,2] = (1,3) \cap X$ and so is also d-open in X.

$(X,d) = ([0,1) \cup \{1 + \frac{1}{n} : n \in \mathbb{N}\}, d_X^{(1)})$,
$A = [0,1]$ and $B = \{1 + \frac{1}{n} : n \in \mathbb{N}\}$.

Clearly $A \cap B = \phi$ and $A \cup B = X$. If $\{A,B\}$ was a disconnection of X, then both A and B would be d-closed. But consider the sequence $(1 + \frac{1}{n})_{n \in \mathbb{N}}$, which $d^{(1)}$-converges to $1 \notin B$. Hence $(1 + \frac{1}{n})$ is a sequence lying in B whose d-limit does not lie in B. Hence B is not d-closed.

We conclude that $\{A,B\}$ is not a disconnection of (X,d).

$(X,d) = (\mathbb{R}, d)$, where d is the discrete metric, $A = \mathbb{Q}$ and $B = \mathbb{R} - \mathbb{Q}$.

Certainly $A \cap B = \phi$ and $A \cup B = X = \mathbb{R}$. In addition, all subsets of X are open for the discrete metric and so both A and B are d-open sets. Hence $\{A,B\}$ is a disconnection for (X,d)

Solution to Question 4

A subspace of $(\mathbb{R}^n, d^{(n)})$ can be homeomorphic to a subset of $(\mathbb{R}^m, d^{(m)})$ if $n \neq m$. Consider, for example, the subspace of $(\mathbb{R}^3, d^{(3)})$ given by $\{(x, y, 0) : x^2 + y^2 \leq 1\}$. This is homeomorphic to the closed unit ball in $(\mathbb{R}^2, d^{(2)})$ given by $\{(x, y) : x^2 + y^2 \leq 1\}$, the homeomorphism being the natural map $h : (x, y, 0) \mapsto (x, y)$.

Alternatively, if $n < m$ then the map $h : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, a_{n+1}, \ldots, a_m)$, where a_i are constants gives a homeomorphism from $\mathbb{R}^n$ to a subspace of $\mathbb{R}^m$.

The correct answer is 'False'.

Solution to Question 5

When determining whether a collection of sets $\mathcal{S}$ forms an open cover of a set A in a metric space (X, d), you must check that both

1. $A \subseteq \bigcup_{U \in \mathcal{S}} U$, and
2. each set $U \in \mathcal{S}$ is d-open.

For the Euclidean metric, the horizontal lines, $A_r = \{(x, r) : x \in \mathbb{R}\}$ are not open but the set of these lines does cover $\mathbb{R}^2$ since any point, $(x, y) \in \mathbb{R}^2$ is in A_y. Therefore the sets form a cover but not an open cover.

The sets B_n are open but do not cover $\mathbb{R}^2$ since $(0, 0) \notin B_n$ for any $n \in \mathbb{N}$.

The open discs, C_n, do not cover the closed disc of radius 2, that is $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$ because the closed disc contains the boundary circle (that is $\{(x, y) : x^2 + y^2 = 4\}$) but this circle of points is not in C_n for any $n \in \mathbb{N}$.

The correct answers are:

$\{A_r : r \in \mathbb{R}\}$ where $A_r = \{(x, r) : x \in \mathbb{R}\}$ is [a cover, which is not open] of $\mathbb{R}^2$ in $(\mathbb{R}^2, d^{(2)})$.

$\{B_n : n \in \mathbb{N}\}$ where $B_n = \{(x, y) : x^2 + y^2 > \frac{1}{n}\}$ is [not a cover] of $\mathbb{R}^2$ in $(\mathbb{R}^2, d^{(2)})$.

$\{C_n : n \in \mathbb{N}\}$ where $C_n = \{(x, y) : x^2 + y^2 < 4 - \frac{1}{n}\}$ is [not a cover] of $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 4\}$ in $(\mathbb{R}^2, d^{(2)})$.

Solution to Question 6

The solution follows Worked Exercise 3.9 of Chapter 22 (Book F page 91).

By Definition 3.8 of Chapter 22 (HB page 130), we need to show that for each $\varepsilon > 0$ we can find a $\delta > 0$ such that for each $f \in A$ and $x, y \in [0, 1]$ we have $|f(x) - f(y)| < \varepsilon$ whenever $|x - y| < \delta$.

(Note that we can use $|\cdot|$ here because the set, A, of functions, is a set of functions in $C[0, 1]$ and these are $(d^{(1)}_{[0,1]}, d^{(1)})$-continuous functions from $[0, 1]$ to $\mathbb{R}$ and so we are working with the usual Euclidean metric.)

Let $\varepsilon > 0$ be given.

Since f is in A we have that $f(x) - f(y) \leq 4|x - y|^{\frac{1}{5}}$.

Hence if $|x - y| < \delta$ then $|f(x) - f(y)| \leq 4\delta^{\frac{1}{5}}$ and so on choosing $\delta = (\frac{1}{2} \times \frac{1}{4}\varepsilon)^5$, we find that for any $f \in A$ we have:

$$\begin{aligned} f(x) - f(y) &\leq 4|x - y|^{\frac{1}{5}} \\ &\leq 4\delta^{\frac{1}{5}} \\ &\leq 4((\tfrac{1}{2} \times \tfrac{1}{4}\varepsilon)^5)^{\frac{1}{5}} \\ &\leq \tfrac{1}{2} \times \varepsilon \\ &\leq \varepsilon. \end{aligned}$$

We conclude that A is an equicontinuous set of functions.

Solution to Question 7

Definition 1.1 of Chapter 16 (HB page 80) defines closed.

This solution follows the solution of Worked Exercise 3.13 of Chapter 22, Book F, page 94.

Let (f_n) be a sequence of functions in A that $d_{\max}$-converges to f. We need to show that $f \in A$. In other words we need to show that $f(\frac{1}{5}) = 4$ and that $|f(x) - f(y)| \leq 3|x - y|^5$ for any $x, y \in [0, 1]$.

Since $f_n \in A$ for all n we have that $f_n(\frac{1}{5}) = 4$ for all n. Since $(f_n) d_{\max}$-converges to f we

know that $(d_{\max}(f_n, f))$ is a null sequence. Therefore we must have $f(\frac{1}{5}) = 4$.

(To see why this is true, note that $|f(\frac{1}{5}) - f_n(\frac{1}{5})| \leq d_{\max}(f, f_n)$ for each n. Therefore since $(d_{\max}(f_n, f))$, is a null sequence then, by the squeeze rule, $(|f(\frac{1}{5}) - f_n(\frac{1}{5})|)$, which is the constant sequence, $(|f(\frac{1}{5}) - 4|)$ must be the zero sequence.)

Now for each $n \in \mathbb{N}$ we have:

$$\begin{aligned} |f(x) - f(y)| &= |f(x) - f_n(x) + f_n(x) \\ &\quad - f_n(y) + f_n(y) - f(y)| \\ &\leq |f(x) - f_n(x)| + |f_n(x) \\ &\quad - f_n(y)| + |f_n(y) - f(y)| \\ &\leq |f_n(x) - f_n(y)| + 2d_{\max}(f_n, f) \\ &\leq 3|x - y|^5 + 2d_{\max}(f_n, f). \end{aligned}$$

However n is arbitrary and $d_{\max}(f_n, f) \to 0$ as $n \to \infty$ so $|f(x) - f(y)| \leq 3|x - y|^5$ for each $x, y \in [0, 1]$.

Hence $f \in A$ and A is $d_{\max}$-closed.

Solution to Question 8

For any metric space (X, d), the set X is both open and closed for d. (See the table on page 89 of the Handbook or Lemma 1.2 and Lemma 2.2 of Chapter 16.)

Hence the set $B = \{\frac{1}{n} : n \in \mathbb{N}\}$ is closed in (B, d_0).

It is also bounded, since we have $d_0(a, b) \leq 1 < 2$ for all $a, b \in B$.

Since all subsets of a discrete metric space are both open and closed (HB page 89), the singleton sets, $\{\frac{1}{n}\}$ (for $n \in \mathbb{N}$), are each open and so $\{\{\frac{1}{n}\} : n \in \mathbb{N}\}$ is an open cover of B that has no finite subcover (since finitely many of these sets can only cover finitely many points and so cannot possibly cover the infinite set B – see also Examples, HB page 132).

Therefore the set B is closed and bounded for d_0 but not compact (by Definitions 4.7 and 4.4 of Chapter 22, HB page 132). Hence (B, d_0) is a closed and bounded metric space that is not compact.

The set $C = \{1, 2, 3, 4, 5\}$ is open in (C, d_0) and bounded, since $d(a, b) \leq 1 < 2$ for all $a, b \in X$. It is also compact since it is finite (HB page 132, Examples). Hence an open bounded metric space can be compact.

By Corollary 5.3 of Chapter 22 (HB page 133) a sequentially compact metric space is bounded, and so an unbounded subset (such as A with the metric induced from the Euclidean metric) cannot be sequentially compact. Hence by Theorem 5.12 of Chapter 22 (HB page 134), such a set is not compact.

The correct answers are:

It is [false] that any closed and bounded metric space is compact. [A counterexample] is given by [(B, d_0), where d_0 is the discrete metric].

It is [false] that an open and bounded metric space is never compact. [A counterexample] is given by [(C, d_0), where d_0 is the discrete metric].

It is [true] that an unbounded metric space is never compact. [An example] is given by [(A, d), where d denotes the metric induced on A by the Euclidean metric].

Solution to Question 9

$(1, \infty)$ is not complete for the metric induced by the Euclidean metric: consider the sequence $(1 + \frac{1}{n})$, it converges (in $(\mathbb{R}, d^{(1)})$) to $1 \notin (1, \infty)$ and so $(1 + \frac{1}{n})_{n \in \mathbb{N}}$ is a $d^{(1)}_{(1,\infty)}$-Cauchy sequence that is not $d^{(1)}_{(1,\infty)}$-convergent.

By the table on page 140 of the HB, $C[0, 1]$ with the $d_{\max}$ metric is complete.

By the table on page 89 of the HB, and Proposition 1.17 of Chapter 16 (HB page 81) $\{f \in C[0, 1] : |f(\frac{1}{2})| = 0 \text{ and } f(x)| \leq 2\}$, being the intersection of two $d_{\max}$-closed sets, is a $d_{\max}$-closed subset of $C[0, 1]$ and so is complete by Proposition 2.2 of Chapter 23 (HB page 136).

The correct answers are:

It is [false] that $(1, \infty)$ with the induced Euclidean metric is a complete metric space.

It is [true] that $\{f \in C[0,1] : |f(\frac{1}{2})| = 0 \text{ and } |f(x)| \leq 2\}$, with the $d_{\max}$ metric, is a complete metric space.

Solution to Question 10

The definition of connectedness is given in Definition 3.1 of Chapter 21 (HB page 120). The definition of compactness is given in Definition 4.7 of Chapter 22 (HB page 132). The definition of completeness is given in Definition 2.1 of Chapter 23 (HB page 136).

For $X = \mathbb{R} - \mathbb{Z}$ and $d = d_0$, we can read off from the table on page 127, that X is (totally) d-disconnected. By the result of Exercise 2.2 of Chapter 23 (or table on page 140 of the HB), we see that (X, d) is complete. (X, d) is not compact – an example of an open cover with no finite subcover is given by $\{\{x\} : x \in X\}$.

For $X = \{\frac{1}{n} : n \in \mathbb{Z} - \{0\}\} \cup \{0\}$ and $d = d_X^{(1)}$, we see that X is a closed subset (for the Euclidean metric) of $\mathbb{R}$.

Hence, since $(\mathbb{R}, d^{(1)})$ is complete (Corollary 2.5 of Chapter 23, HB page 136), Proposition 2.2 of Chapter 23 (HB page 136) implies that (X, d) is complete. In addition X is a bounded subset of $\mathbb{R}$ for the Euclidean metric. Hence by the Heine-Borel Theorem (Theorem 2.3 or Theorem 2.12 of Chapter 22, HB pages 128 and 129), X is d-sequentially compact and hence, by Theorem 5.12 of Chapter 23 (HB page 134), (X, d) is compact. Finally (X, d) is disconnected and a disconnection is given by $\{A, B\}$, where $A = \{-1\}$ and $B = X - A$.

For $X = \mathbb{R}^2 - \mathbb{Q}^2$ and $d = d^{(1)}_{\mathbb{R}^2 - \mathbb{Q}^2}$, since $\mathbb{Q}^2$ is countable, we conclude from the table on page 127 of the Handbook that (X, d) is (path-) connected. However X is not a closed subset of the plane with the Euclidean metric and so, by the Heine-Borel Theorem (Theorem 2.12 of Chapter 22, HB page 129) is not sequentially compact for d and so, by Theorem 5.12 of Chapter 23 (HB page 134) it is not compact.

By considering a sequence such as $(\mathbf{a}_n)$, where $\mathbf{a}_n = \left(\frac{\sqrt{2}}{n}, 0\right)$ (which has limit $(0,0)$), we see that there are Cauchy sequences in X that are not convergent to a point in X. We conclude that (X, d) is not complete.

The correct answer is:

Set	**Metric**, d	d -connected?	d -compact?	d -complete?
$(\mathbb{R} - \mathbb{Z})$	d_0	[no]	[no]	[yes]
$X = \{\frac{1}{n} : n \in \mathbb{Z} - \{0\}\} \cup \{0\}$	$d_X^{(1)}$	[no]	[yes]	[yes]
$\mathbb{R}^2 - \mathbb{Q}^2$	$d^{(1)}_{\mathbb{R}^2 - \mathbb{Q}^2}$	[yes]	[no]	[no]

Solution to Question 11

We use the definition of the Hausdorff metric given in Chapter 24, Definition 2.10 (HB page 142) and recall that

$$d_H(A, B) = \max\{d^{(2)}(A, B), d^{(2)}(B, A)\},$$

where

$$d^{(2)}(A, B) = \max\{d^{(2)}((x, y), B) : (x, y) \in A\},$$

and

$$d^{(2)}(B, A) = \max\{d^{(2)}((x, y), A) : (x, y) \in B\}.$$

Since $d^{(2)}((x, y), A) = \min\{d^{(2)}((x, y), \mathbf{c}) : \mathbf{c} \in C\}$, for any set C, we find that

$$d^{(2)}(A, B) = 3$$

and

$$d^{(2)}(B, A) = 3.$$

Hence $d_H(A, B) = \max\{3, 3\} = 3$.

Solution to Question 12

We follow the method described in Chapter 24.

First we note that the open set condition holds (Definition 3.4 of Chapter 24, HB page 143): taking $U = (0, 1)$, we find that $S_1(U) = (0, \frac{1}{9})$, $S_2(U) = (\frac{1}{3}, \frac{2}{3})$, and $S_3(U) = (\frac{2}{3}, 1)$ and these intervals are disjoint and contained in U.

Hence, by Theorem 3.5 of Chapter 24 (HB page 143), the dimension of K is given by the (unique) s that satisfies

$$\frac{2}{3^s} + \frac{1}{3^{2 \cdot s}} = 1,$$

or, equivalently,

$$\frac{2}{3^s} + \frac{1}{3^{2 \cdot s}} - 1 = 0,$$

On making the substitution $x = (\frac{1}{3})^s$, we obtain

$$x^2 + 2 \cdot x - 1 = 0$$

and solving this quadratic equation for x gives

$$x = -\sqrt{2} - 1 \text{ or } x = \sqrt{2} - 1$$

but $s > 0$ and so $x > 0$ and we conclude that $x = \sqrt{2} - 1$, implying that $\dim(K) = s = -\frac{\log(\sqrt{2}-1)}{\log(3)} = \frac{\log(\sqrt{2}+1)}{\log(3)}$.